

Best Available Copy

PCT/JP2004/012226

日本国特許庁 19.08.2004
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2003年 8月20日

出願番号 Application Number: 特願2003-296001

[ST. 10/C]: [JP2003-296001]

出願人 Applicant(s): 松下電器産業株式会社

REC'D 07 OCT 2004
WIPO PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 9月24日

特許庁長官
Commissioner,
Japan Patent Office

小川

洋

【書類名】 特許願
【整理番号】 2022550076
【提出日】 平成15年 8月20日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 17/00
【発明者】
【住所又は居所】 大阪府門真市大字門真 1006番地
【氏名】 山道 将人
【発明者】
【住所又は居所】 大阪府門真市大字門真 1006番地
【氏名】 大森 基司
【発明者】
【住所又は居所】 大阪府門真市大字門真 1006番地
【氏名】 山本 雅哉
【発明者】
【住所又は居所】 大阪府門真市大字門真 1006番地
【氏名】 渡▲なべ▼ 和久
【発明者】
【住所又は居所】 大阪府門真市大字門真 1006番地
【氏名】 佐草 敦
【発明者】
【住所又は居所】 大阪府門真市大字門真 1006番地
【氏名】 山本 尚明
【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社
【代理人】
【識別番号】 100090446
【弁理士】
【氏名又は名称】 中島 司朗
【手数料の表示】
【予納台帳番号】 014823
【納付金額】 21,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9003742

【書類名】特許請求の範囲**【請求項 1】**

コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを配信するコンテンツ提供装置と、

前記マスタ鍵を示すマスタ情報を記憶しているコンテンツ利用記録媒体と、

前記コンテンツ提供装置より前記暗号化コンテンツと前記暗号化コンテンツ鍵とを取得し、前記コンテンツ利用記録媒体に記録されている前記マスタ情報をからマスタ鍵を生成し、生成したマスタ鍵を用いて、前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う再生装置と

から構成されることを特徴とするコンテンツ再生システム。

【請求項 2】

前記コンテンツ利用記録媒体は、前記再生装置に固有のデバイス鍵を用いて、前記マスタ鍵が暗号化された暗号化マスタ鍵を含む前記マスタ情報を記憶しており、

前記再生装置は、固有のデバイス鍵を用いて、前記暗号化マスタ鍵を復号して、マスタ鍵を生成する

ことを特徴とする請求項 1 に記載のコンテンツ再生システム。

【請求項 3】

コンテンツ利用記録媒体とコンテンツ提供装置とからコンテンツを取得し、取得したコンテンツの再生を制御する再生装置であつて、

前記コンテンツ提供装置より、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを取得するコンテンツ情報取得手段と

、
コンテンツの再生を許可する場合に、前記コンテンツ利用記録媒体に記憶されている前記マスタ鍵を示すマスタ情報をからマスタ鍵を生成し、生成したマスタ鍵を用いて、取得した前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成するコンテンツ鍵生成手段と

、
生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号して、コンテンツを生成するコンテンツ生成手段と、

生成した前記コンテンツの再生を行う再生手段と
を備えることを特徴とする再生装置。

【請求項 4】

前記コンテンツ利用記録媒体が有する前記マスタ情報は、前記再生装置に固有のデバイス鍵を用いて、前記マスタ鍵が暗号化された暗号化マスタ鍵を含み、

前記コンテンツ鍵生成手段は、固有のデバイス鍵を用いて、前記暗号化マスタ鍵を復号して、マスタ鍵を生成する

ことを特徴とする請求項 3 に記載の再生装置。

【請求項 5】

前記コンテンツ利用記録媒体は、さらに、コンテンツの利用期間を示す利用期間情報を、前記マスタ情報と対応付けて記憶しており、

前記コンテンツ情報取得手段は、さらに、取得するコンテンツをレンタルにて取得すること、若しくは購入にて取得することを示す取得情報を受け付ける取得方法受付手段と、前記取得方法受付手段にて受け付けた取得情報を、取得した暗号化コンテンツ及び暗号化コンテンツ鍵と対応付けて格納する格納手段とを備え、

前記コンテンツ鍵生成手段は、さらに、取得情報がレンタルを示すか、購入を示すかの判断を行う取得情報判断手段と、購入を示すと判断する場合には、コンテンツの再生を許可し、レンタルを示すと判断する場合には、コンテンツの利用が期間内であれば、コンテンツの再生を許可する再生判断手段とを備える

ことを特徴とする請求項3に記載の再生装置。

【請求項6】

前記再生判断手段は、さらに、

コンテンツの再生指示を受け付ける再生受付手段と、

前記取得情報判断手段にて、取得情報がレンタルを示すと判断する場合に、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵の取得から、前記再生指示を受け付けるまでの期間を算出し、算出した期間が、前記利用期間内であるか否かの判断を行う期間判断手段を備える

ことを特徴とする請求項5に記載の再生装置。

【請求項7】

前記コンテンツ利用記録媒体は、さらに、前記コンテンツ提供者より取得可能なコンテンツの条件を示す利用可能コンテンツ情報を記憶しており、

前記コンテンツ情報取得手段は、条件を満たすか否かを判断し、条件を満たす場合には、暗号化コンテンツと暗号化コンテンツ鍵とを取得し、条件を満たさない場合には、暗号化コンテンツと暗号化コンテンツ鍵とを取得しない

ことを特徴とする請求項5に記載の再生装置。

【請求項8】

前記コンテンツ提供装置は、暗号化コンテンツ及び暗号化コンテンツ鍵を、コンテンツ配信要求の有無に関わらず配信を行っており、

前記コンテンツ情報取得手段は、前記コンテンツ提供装置より暗号化コンテンツ及び暗号化コンテンツ鍵を受信し、受信した暗号化コンテンツ及び暗号化コンテンツ鍵が、前記利用可能コンテンツ情報に示された条件を満たすか否かを判断し、前記受信判断手段が条件を満たすと判断する場合には、受信した暗号化コンテンツ及び暗号化コンテンツ鍵を取得し、条件を満たさない場合には、受信した暗号化コンテンツ及び暗号化コンテンツ鍵を破棄する

ことを特徴とする請求項7に記載の再生装置。

【請求項9】

複数のコンテンツに共通であり、且つコンテンツ鍵を暗号化するマスタ鍵を示すマスタ情報を、コンテンツの利用期間を示す利用期間情報と対応付けて記憶している

ことを特徴とするコンテンツ利用記録媒体。

【請求項10】

前記マスタ情報を、さらに、前記コンテンツ提供者より取得可能なコンテンツの条件を示す利用可能コンテンツ情報と対応付けて記憶している

ことを特徴とする請求項9に記載のコンテンツ利用記録媒体。

【請求項11】

前記コンテンツ利用記録媒体が記憶しているマスタ情報を、コンテンツを再生する再生装置に固有のデバイス鍵を用いて、前記マスタ鍵が暗号化された暗号化マスタ鍵を含む

ことを特徴とする請求項9に記載のコンテンツ利用記録媒体。

【請求項12】

再生装置とネットワークを介して接続されたコンテンツ提供装置であって、

コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通であり、利用が許可されているマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを記憶しているコンテンツ情報記憶手段と、

前記コンテンツ情報記憶手段にて記憶している前記暗号化コンテンツ及び前記暗号化コンテンツ鍵を、ネットワークを介して前記再生装置へ配信を行う配信手段とを備えることを特徴とするコンテンツ提供装置。

【請求項13】

前記コンテンツ提供装置は、さらに、

複数のマスタ鍵を記憶しているマスタ鍵記憶手段と、

前記複数のマスタ鍵のうち利用を許可しないマスタ鍵を利用不可状態とする状態変更手段と、

前記複数のマスタ鍵のうち利用が許可された少なくとも1個以上のマスタ鍵を用いて、マスタ鍵に対応する暗号化コンテンツ鍵を生成するコンテンツ鍵暗号化手段とを備えることを特徴とする請求項12に記載のコンテンツ提供装置。

【請求項14】

コンテンツ利用記録媒体にデータを書き込むデータ書込装置であって、

複数のコンテンツに共通であり、且つコンテンツ鍵を暗号化するマスタ鍵を生成するマスタ鍵生成手段と、

前記マスタ鍵を示すマスタ情報を生成するマスタ情報生成手段と、

生成したマスタ情報を前記コンテンツ利用記録媒体へ書き込む書込手段とを備えることを特徴とするデータ書込装置。

【請求項15】

コンテンツ利用記録媒体とコンテンツ提供装置とからコンテンツを取得し、取得したコンテンツの再生を制御する再生装置に用いられるコンテンツ再生方法であって、

前記コンテンツ提供装置より、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを取得するコンテンツ情報取得ステップと、

コンテンツの再生を許可する場合に、前記コンテンツ利用記録媒体に記憶されている前記マスタ鍵を示すマスタ情報をからマスタ鍵を生成し、生成したマスタ鍵を用いて、取得した前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成するコンテンツ鍵生成ステップと、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号して、コンテンツを生成するコンテンツ生成ステップと、

生成した前記コンテンツの再生を行う再生ステップとを含むことを特徴とするコンテンツ再生方法。

【請求項16】

コンテンツ利用記録媒体とコンテンツ提供装置とからコンテンツを取得し、取得したコンテンツの再生を制御する再生装置に用いられるコンテンツ再生プログラムであって、

前記コンテンツ提供装置より、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを取得するコンテンツ情報取得ステップと、

コンテンツの再生を許可する場合に、前記コンテンツ利用記録媒体に記憶されている前記マスタ鍵を示すマスタ情報をからマスタ鍵を生成し、生成したマスタ鍵を用いて、取得した前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成するコンテンツ鍵生成ステップと、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号して、コンテンツを生成するコンテンツ生成ステップと、

生成した前記コンテンツの再生を行う再生ステップとを含むことを特徴とするコンテンツ再生プログラム。

【請求項17】

コンテンツ利用記録媒体とコンテンツ提供装置とからコンテンツを取得し、取得したコンテンツの再生を制御する再生装置に用いられるコンテンツ再生プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記コンテンツ再生プログラムは、

前記コンテンツ提供装置より、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを取得するコンテンツ情報取得ステッ

と、

コンテンツの再生を許可する場合に、前記コンテンツ利用記録媒体に記憶されている前記マスタ鍵を示すマスタ情報からマスタ鍵を生成し、生成したマスタ鍵を用いて、取得した前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成するコンテンツ鍵生成ステップと、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号して、コンテンツを生成するコンテンツ生成ステップと、

生成した前記コンテンツの再生を行う再生ステップと
を含むことを特徴とする記録媒体。

【書類名】明細書

【発明の名称】コンテンツ再生システム、コンテンツ利用記録媒体、再生装置、コンテンツ提供装置及びデータ書き込み装置

【技術分野】

【0001】

本発明は、利用者の前払い金額の範囲内にて、音楽、映像、プログラム等のコンテンツをネットワークを介して受信し、利用する技術に関する。

【背景技術】

【0002】

近年、ADSL等の広帯域ネットワークの普及により、利用者は、音楽、映像、プログラム等のコンテンツをコンテンツ提供者よりネットワークを通じて購入することが可能となっている。また、コンテンツ購入時には、コンテンツ提供者より配信されるコンテンツは、著作権等の問題により、暗号化されて配信されている。利用者は、暗号化されたコンテンツを復号して、コンテンツを利用する。

【0003】

ネットワークを通じてコンテンツを購入する際、コンテンツ購入料金に対する決済を行う必要があり、この決済方法として、銀行口座やクレジットカード番号をSSL等のPKI (Public Key Infrastructure) を利用して送信し、決済を行う方法や、ユーザの利用料金をコンテンツ提供者にて管理し、後日請求する決済方法が用いられている。

【0004】

前者の方法では、銀行口座やクレジットカード番号が、不正な第三者により不正な手段にて盗聴されることも考えられ、後者の方では、ユーザの利用料金の管理及び、請求するための仕組みを備える必要があり、コンテンツ提供者が有するシステムが複雑となる。

【0005】

そこで、特許文献1にて、従来より簡単な決済方法を用いることができるプリペイド記録媒体が開示されている。このプリペイド記録媒体は、データの書き込み可能な不揮発性半導体メモリカードまたは光あるいは磁気記録ディスク等のカード型記録媒体であって、配信センターから配信される各種コンテンツ情報を書き込み記録する際に生じる課金金額を予め前払いし、その前払い済課金データを記録するプリペイド情報記憶領域と、前記配信センターから配信された各種コンテンツ情報を書き込み記録するコンテンツ情報記録領域と、暗号化されたコンテンツに対する暗号解読キーを備える領域とを具備している。これによると、予め前払いした課金金額の範囲内で、暗号解読キーに対応する暗号化されたコンテンツのダウンロードやコピーが可能となる。

【特許文献1】特開2001-60286号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

一般に、コンテンツの暗号化に用いられる暗号化鍵と、その暗号化鍵に対応する復号鍵とは、コンテンツ毎に異なっている。

【0007】

上記に示すプリペイド記録媒体は、暗号解読キーにて復号できるコンテンツのみをダウンロード又はコピーすることができる。そのため、このプリペイド記録媒体の購入時には、コンテンツ提供者よりダウンロード又はコピーして利用するコンテンツを決定しておく必要がある。つまり、利用できるコンテンツは、プリペイド記録媒体に記録された暗号解読キーに依存している。

【0008】

これでは、プリペイドカードが持つ、前払い金額の範囲内でコンテンツを自由に購入できるという利点が生かせないことになる。

【0009】

そこで、本発明では、利用者が所有する情報に依存することなく、自由にコンテンツをレンタル又は購入し、再生を行うことができるコンテンツ再生システム、コンテンツ利用記録媒体、再生装置、コンテンツ提供装置、データ書き込み装置、コンテンツ再生方法、プログラム及び記録媒体を提供することを目的とする。

【課題を解決するための手段】

【0010】

上記目的を達成するために、本発明は、コンテンツ再生システムであって、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを配信するコンテンツ提供装置と、前記マスタ鍵を示すマスタ情報を記憶しているコンテンツ利用記録媒体と、前記コンテンツ提供装置より前記暗号化コンテンツと前記暗号化コンテンツ鍵とを取得し、前記コンテンツ利用記録媒体に記録されている前記マスタ情報からマスタ鍵を生成し、生成したマスタ鍵を用いて、前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う再生装置とから構成される。

【発明の効果】

【0011】

本発明は、コンテンツ再生システムであって、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを配信するコンテンツ提供装置と、前記マスタ鍵を示すマスタ情報を記憶しているコンテンツ利用記録媒体と、前記コンテンツ提供装置より前記暗号化コンテンツと前記暗号化コンテンツ鍵とを取得し、前記コンテンツ利用記録媒体に記録されている前記マスタ情報からマスタ鍵を生成し、生成したマスタ鍵を用いて、前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う再生装置とから構成される。

【0012】

この構成によると、コンテンツ利用記録媒体に記憶しているマスタ情報は、コンテンツに依存していない。そのため、利用者は、マスタ情報に依存することなく、暗号化コンテンツよりコンテンツを生成し、利用することができる。

【0013】

ここで、前記コンテンツ利用記録媒体は、前記再生装置に固有のデバイス鍵を用いて、前記マスタ鍵が暗号化された暗号化マスタ鍵を含む前記マスタ情報を記憶しており、前記再生装置は、固有のデバイス鍵を用いて、前記暗号化マスタ鍵を復号して、マスタ鍵を生成するとしてもよい。

【0014】

この構成によると、マスタ情報をデバイス鍵にて暗号化することにより、コンテンツ記録媒体のセキュリティが向上する。

【0015】

また、本発明は、コンテンツ利用記録媒体とコンテンツ提供装置とからコンテンツを取得し、取得したコンテンツの再生を制御する再生装置であって、前記コンテンツ提供装置より、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通のマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを取得するコンテンツ情報取得手段と、コンテンツの再生を許可する場合に、前記コンテンツ利用記録媒体に記憶されている前記マスタ鍵を示すマスタ情報をからマスタ鍵を生成し、生成したマスタ鍵を用いて、取得した前記暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成するコンテンツ鍵生成手段と、生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号して、コンテンツを生成するコンテンツ生成手段と、生成した前記コンテンツの再生を行う再生手段とを備える。

【0016】

この構成によると、再生装置は、コンテンツの再生を許可する場合に、コンテンツ利用記録媒体に記憶されているマスタ情報を用いて、コンテンツ提供装置より配信された暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生することができる。

【0017】

ここで、前記コンテンツ利用記録媒体は、さらに、コンテンツの利用期間を示す利用期間情報を、前記マスタ情報を対応付けて記憶しており、前記コンテンツ情報取得手段は、さらに、取得するコンテンツをレンタルにて取得すること、若しくは購入にて取得することを示す取得情報を受け付ける取得方法受付手段と、前記取得方法受付手段にて受け付けた取得情報を、取得した暗号化コンテンツ及び暗号化コンテンツ鍵と対応付けて格納する格納手段とを備え、前記コンテンツ鍵生成手段は、さらに、取得情報がレンタルを示すか、購入を示すかの判断を行う取得情報判断手段と、購入を示すと判断する場合には、コンテンツの再生を許可し、レンタルを示すと判断する場合には、コンテンツの利用が期間内であれば、コンテンツの再生を許可する再生判断手段とを備えるとしてもよい。

【0018】

この構成によると、再生判断手段にて、取得情報が購入を示すか、レンタルを示すかの判断を行っている。これにより、コンテンツの取得情報に応じた再生判断を行うことが可能となる。

【0019】

ここで、前記再生判断手段は、さらに、コンテンツの再生指示を受け付ける再生受付手段と、前記取得情報判断手段にて、取得情報がレンタルを示すと判断する場合に、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵の取得から、前記再生指示を受け付けるまでの期間を算出し、算出した期間が、前記利用期間内であるか否かの判断を行う期間判断手段を備えるとしてもよい。

【0020】

この構成によると、取得情報がレンタルを示す場合、暗号化コンテンツ及び暗号化コンテンツ鍵を取得してから再生指示を受け付けるまでの期間を算出し、算出した期間と、コンテンツ利用記録媒体に記憶している利用期間とを用いて、コンテンツの再生の許可を判断することが可能となる。

【0021】

また、本発明は、複数のコンテンツに共通であり、且つコンテンツ鍵を暗号化するマスタ鍵を示すマスタ情報を、コンテンツの利用期間を示す利用期間情報と対応付けて記憶していることを特徴とするコンテンツ利用記録媒体である。

【0022】

この構成によると、コンテンツ利用記録媒体は、マスタ情報を利用期間と対応付けて記憶している。これにより、マスタ情報の利用期間を制限することができる。

【0023】

ここで、前記マスタ情報を、さらに、前記コンテンツ提供者より取得可能なコンテンツの条件を示す利用可能コンテンツ情報と対応付けて記憶しているとしてもよい。

【0024】

この構成によると、コンテンツ利用記録媒体は、さらに、マスタ情報を取得可能なコンテンツの条件と対応付けて記憶している。これにより、取得可能なコンテンツを抽出することができる。

【0025】

ここで、前記コンテンツ利用記録媒体が記憶しているマスタ情報は、コンテンツを再生する再生装置に固有のデバイス鍵を用いて、前記マスタ鍵が暗号化された暗号化マスタ鍵を含むとしてもよい。

【0026】

この構成によると、マスタ情報をデバイス鍵にて暗号化することにより、コンテンツ記録媒体のセキュリティが向上する。

【0027】

また、本発明は、再生装置とネットワークを介して接続されたコンテンツ提供装置であって、コンテンツに固有のコンテンツ鍵を用いて、コンテンツが暗号化された暗号化コンテンツと、複数のコンテンツに共通であり、利用が許可されているマスタ鍵を用いて、前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵とを記憶しているコンテンツ情報記憶手段と、前記コンテンツ情報記憶手段にて記憶している前記暗号化コンテンツ及び前記暗号化コンテンツ鍵を、ネットワークを介して前記再生装置へ配信を行う配信手段とを備える。

【0028】

この構成によると、コンテンツ提供装置は、再生装置へ暗号化コンテンツと暗号化コンテンツ鍵とを配信することが可能となる。

【0029】

また、本発明は、コンテンツ利用記録媒体にデータを書き込むデータ書込装置であって、複数のコンテンツに共通であり、且つコンテンツ鍵を暗号化するマスタ鍵を生成するマスタ鍵生成手段と、前記マスタ鍵を示すマスタ情報を生成するマスタ情報生成手段と、生成したマスタ情報を前記コンテンツ利用記録媒体へ書き込む書込手段とを備える。

【0030】

この構成によると、データ書込装置は、コンテンツ利用記録媒体へ、複数のコンテンツに共通のマスタ鍵を示すマスタ情報を書き込むことが可能となる。

【発明を実施するための最良の形態】

【0031】

1. 第1の実施の形態

本発明に係る第1の実施の形態としてのプリペイドカードシステム1について説明する。

【0032】

1. 1 プリペイドカードシステム1の構成

ここでは、プリペイドカードシステム1の構成について説明する。

【0033】

プリペイドカードシステム1は、図1に示す第1サブシステム10、11、…、12及び第2サブシステム20とから構成される。第1サブシステム10は、記録媒体100と、記録媒体100の着脱が可能な再生装置200とから構成される。ここで、記録媒体100は、DVD-RAMなどの光ディスクである。なお、第1サブシステム11、…、12は、第1サブシステム10と同様の構成である。第2サブシステム20は、ライセンスチケット生成装置300とコンテンツ提供装置400とから構成され、ライセンスチケット生成装置300とコンテンツ提供装置400とは、専用線を用いてネットワーク接続されている。また、コンテンツ提供装置400と、第1サブシステム10、11、…、12が有する各再生装置とは、インターネットを介してネットワーク接続が可能となっている。

【0034】

また、再生装置200は、利用者からの情報を受け付けるためのリモコン及び入力部と、コンテンツ提供装置とインターネットを介して情報を送受信するための第1入出力部と、記録媒体100に対して情報を入出力するための第2入出力部とを備え、さらに、再生装置200は、テレビに接続され、コンテンツなどのデータを接続されたテレビに出力するための出力部をも備えている。

【0035】

第1サブシステムは、利用者側のサブシステムであり、第2サブシステムは、コンテンツ提供者側のサブシステムである。ここでは、コンテンツ提供者は、映画会社とする。

【0036】

ここで、プリペイドカードシステム1における各装置間の関係を、記録媒体100と再生装置200とライセンスチケット生成装置300とコンテンツ提供装置400とを用いて、簡単に説明する。

【0037】

先ず、ライセンスチケット生成装置300において、コンテンツ提供装置400よりコンテンツのレンタル又は購入する際に、利用される情報を生成し、生成した情報を記録媒体へ書き込み、記録媒体100が生成される。また、コンテンツ提供装置400において、コンテンツの暗号化と、コンテンツの暗号化に利用したコンテンツ鍵の暗号化が行われ、暗号化されたコンテンツと暗号化されたコンテンツ鍵とが記憶されている。

【0038】

ライセンスチケット生成装置300において生成された記録媒体100は、販売店にて販売され、利用者は、販売店より、記録媒体100を購入することとなる。なお、記録媒体100にて、コンテンツのレンタル又は購入ができる料金を前払いにて、記録媒体100の購入時に支払っておく。

【0039】

利用者は、購入した記録媒体100を再生装置200へ装着し、さらに、コンテンツ提供装置400とネットワーク接続を行い、記録媒体100に記録されている情報を用いて、コンテンツのレンタル又は購入したいコンテンツの要求をコンテンツ提供装置400に対して行う。

【0040】

コンテンツ提供装置400は、再生装置200よりコンテンツの要求を受けると、要求のあったコンテンツに対する暗号化されたコンテンツ及び暗号化されたコンテンツ鍵を送信する。再生装置200は、コンテンツに係る情報を受信し、記録媒体100へ記録する。

【0041】

利用者は、再生を行う場合には、記録媒体100を再生装置200へ装着して、再生を行う。

【0042】

なお、記録媒体100は、インターネットによるオンラインショッピングにて購入してもよい。

【0043】

なお、以降では、暗号化されたコンテンツを暗号化コンテンツと呼び、暗号化されたコンテンツ鍵を暗号化コンテンツ鍵と呼ぶ。

【0044】

また、第1サブシステム11、12とライセンスチケット生成装置300とコンテンツ提供装置400における装置間の関係も上記と同様であるため、説明は省略する。

【0045】

1.2 記録媒体100の構成

ここでは、記録媒体100の構成について説明する。

【0046】

記録媒体100は、図2に示すROM領域101とRAM領域102とから構成されている。ROM領域101は、読み出しのみが可能な領域であり、ライセンスチケット記憶部110と配信要求機能記憶部120とを有している。RAM領域102は、読み出し及び書き込みが可能な領域であり、コンテンツ記憶部130と利用状況記憶部140とを有している。

【0047】

以下において、ライセンスチケット記憶部110、コンテンツ記憶部130、利用状況記憶部140及び配信要求機能記憶部120についての説明を行う。なお、第1サブシステム11、12が有する記録媒体は、記録媒体100と同様の構成を有している

ため、説明は省略する。

【0048】

1. 2. 1 ライセンスチケット記憶部110

ライセンスチケット記憶部110は、図3に一例として示すように、ライセンスチケットテーブルT100を有している。

【0049】

ライセンスチケットテーブルT100は、チケット番号、利用可能コンテンツID、利用規則、及びチケット用暗号化マスタ鍵からなる組を1個以上記憶するための領域を備えている。また、チケット番号、利用可能コンテンツID、利用規則、及びチケット用暗号化マスタ鍵からなる組をライセンスチケットという。なお、本実施の形態では、ライセンスチケットの数を10とする。

【0050】

チケット番号は、ライセンスチケットテーブルT100に記録されている1個以上のライセンスチケットに割り当てられる番号である。

【0051】

利用可能コンテンツIDは、利用者が、コンテンツ提供装置400より、レンタル又は購入できるコンテンツIDが記録されている。ここで、コンテンツIDは、コンテンツごとに付加される識別子であり、7桁の数字から構成されている。先頭3桁は、コンテンツを提供する映画会社を識別する映画会社識別子であり、残り4桁は、作品を識別する作品識別子である。

【0052】

なお、利用可能コンテンツIDに記録されるコンテンツIDに含まれる作品識別子は、ワイルドカード表記が可能である。例えば、コンテンツIDが「100****」と記録されている場合には、映画会社識別子「100」に対応するコンテンツ提供会社が有する任意のコンテンツのレンタル又は購入が可能であることを示す。また、コンテンツIDが「1000***」と記録されている場合には、映画会社識別子「100」に対応するコンテンツ提供会社が有するコンテンツのうち、作品識別子の先頭1桁が「0」であるコンテンツより任意のコンテンツのレンタル又は購入が可能であることを示す。また、「100001」と記録されている場合には、映画会社識別子「100」に対応するコンテンツ提供会社が有するコンテンツのうち、作品識別子が「0001」であるコンテンツのレンタル又は購入が可能であることを示す。

【0053】

利用規則は、レンタルと購入とからなる組で構成されている。レンタルは、利用者が、コンテンツ提供装置400より、コンテンツをレンタルする場合のレンタル期間を示す。また、購入は、コンテンツ提供装置400より、コンテンツを購入する場合の利用可能な金額を示す。

【0054】

チケット用暗号化マスタ鍵は、再生装置200に予め記憶されているデバイス鍵「DK」にて、コンテンツを暗号化する際に用いられるコンテンツ鍵を暗号化するマスタ鍵「WK」を共通鍵暗号で暗号化した情報である。

【0055】

ここで、共通鍵暗号とは、ある情報の暗号化及び復号において、同一の鍵を用いて行うことであり、一例として、DESである。DESについては、公知であるので説明を省略する。また、暗号鍵Aで情報Bを共通鍵暗号で、暗号化したものを、Enc(A, B)と表記する。例えば、デバイス鍵「DK」で、マスタ鍵「WK」を共通鍵暗号で、暗号化した暗号化マスタ鍵は、Enc(DK, WK)と表記される。

【0056】

なお、ライセンスチケットテーブルT100の各ライセンスチケットに含まれる利用可能コンテンツIDの先頭3桁には、同一の値が記録されている。つまり、1つの記録媒体100で複数の映画会社からコンテンツのレンタル又は購入はできない。

【0057】

また、本実施の形態では、記録媒体100の購入時に、前払いとして支払う料金は、各ライセンスチケットの利用規則に記録されている金額の合計とする。

【0058】

1. 2. 2 コンテンツ記憶部130

コンテンツ記憶部130は、図4に示すように、レンタルコンテンツ記憶部131と、購入コンテンツ記憶部132とを有している。

【0059】

レンタルコンテンツ記憶部131は、コンテンツ提供装置400より、コンテンツをレンタルにて、受信したコンテンツに係る情報を記憶している。ここでは、暗号化コンテンツ鍵と暗号化コンテンツとの組からなる情報と、コンテンツIDとを対応付けて記憶している。

【0060】

購入コンテンツ記憶部132は、コンテンツ提供装置400より、購入したコンテンツに係る情報を記憶している。ここでは、コンテンツIDと、コンテンツのデータとを対応付けて記憶している。

【0061】

なお、図4にて用いられている「C N T n」（nは数字）は、コンテンツを示し、「C K n」（nは数字）は、コンテンツ鍵を示している。例えば、「C N T 1」は、コンテンツID「1000001」に対応するコンテンツであることを示し、「C K 1」は、コンテンツ「C N T 1」を暗号化する際に用いられるコンテンツ鍵であることを示す。また、異なるコンテンツに対して、異なるコンテンツ鍵が割り当てられている。

【0062】

1. 2. 3 利用状況記憶部140

利用状況記憶部140は、図5に示すように、利用状況テーブルT150を有している。

【0063】

利用状況テーブルT150は、ライセンスチケット記憶部110に記録されているライセンスチケットの利用状況を示しており、利用番号、利用状態、利用形態、利用開始日時、コンテンツID、コンテンツ名及び定価からなる組を1個以上記憶するための領域を備えている。また、利用番号、利用状態、利用形態、利用開始日時、コンテンツID、コンテンツ名及び定価からなる組をライセンスチケット利用情報という。なお、ライセンスチケット利用情報の数は、ライセンスチケットの数となる。

【0064】

利用番号は、ライセンスチケット利用情報に割り当てられた番号であり、ライセンスチケットのチケット番号と対応している。なお、利用番号は、予め記録されている。

【0065】

利用状態は、利用番号に対応するチケット番号のライセンスチケットの利用状況を示し、「未利用」、「利用中」、「利用済」の何れかが、記録されている。「未利用」は、利用番号に対応するチケット番号のライセンスチケットが利用されていないことを示し、「利用中」は、利用番号に対応するチケット番号のライセンスチケットにてレンタルされたコンテンツが、レンタル中であることを示し、「利用済」は、利用番号に対応するチケット番号のライセンスチケットにてレンタルされたコンテンツのレンタル期間が過ぎたこと又は、利用番号に対応するチケット番号のライセンスチケットにてコンテンツが購入されたことを示している。なお、記録媒体100の購入時には、利用状態は、「未利用」となっている。

【0066】

利用開始日時は、コンテンツ提供装置400より、受信した配信コンテンツ情報の受信完了を示す年月日及び時分を記録している。コンテンツをレンタルした場合には、利用開始日時に記録された年月日及び時分を基準として、レンタル期間が過ぎたか否かを判断す

る。なお、記録媒体100の購入時には、利用開始日時は、空白である。

【0067】

コンテンツIDは、利用番号に対応するチケット番号のライセンスチケットを用いて、レンタル又は購入されたコンテンツのコンテンツIDが記録されている。なお、記録媒体100の購入時には、コンテンツIDは、空白である。

【0068】

コンテンツ名は、利用番号に対応するチケット番号のライセンスチケットを用いて、レンタル又は購入されたコンテンツのコンテンツ名が記録されている。なお、記録媒体100の購入時には、コンテンツ名は、空白である。

【0069】

定価は、利用番号に対応するチケット番号のライセンスチケットを用いて、レンタル又は購入されたコンテンツの定価を示す。なお、記録媒体100の購入時には、定価は、空白である。

【0070】

なお、本実施の形態では、利用開始日時には、年月日及び時分の記録としているが、これに限定はされない。利用開始日時に記録された情報を基準として、レンタル期間が過ぎたか否かの判断が可能であればよい。

【0071】

1. 2. 4 配信要求機能記憶部120

配信要求機能記憶部120は、取得可能コンテンツ一覧画面情報、利用形態選択画面情報、レンタル用チケット選択画面情報、購入用チケット選択画面情報、及び配信要求プログラムを記憶している。

【0072】

配信要求プログラムは、再生装置200にて読み出され、実行される。

【0073】

(A) 取得可能コンテンツ一覧画面情報

取得可能コンテンツ一覧画面情報は、図6に一例として示す取得可能コンテンツ一覧画面M100を生成するための情報である。取得可能コンテンツ一覧画面M100は、ライセンスチケットにて、レンタル又は購入可能なコンテンツの情報を表示するために用いられる画面であり、レンタル又は購入可能なコンテンツを示す取得可能コンテンツ一覧情報に含まれる管理コンテンツ情報を表示する。ここで、管理コンテンツ情報は、コンテンツごとに付加される識別子であるコンテンツID、コンテンツ名及びコンテンツの定価から構成される情報である。また、図6において、反転表示されている管理コンテンツ情報は、現在、選択されている管理コンテンツ情報を示す。

【0074】

利用者は、取得可能コンテンツ一覧画面M100より、レンタル又は購入したいコンテンツの選択を行うことができる。

【0075】

(B) 利用形態選択画面情報

利用形態選択画面情報は、図7に一例として示す利用形態選択画面M150を生成及び制御する。利用形態選択画面M150は、取得可能コンテンツ一覧画面M100にて選択されたコンテンツに対して、レンタルか又は、購入するかの選択を受け付けるために用いる画面である。利用形態選択画面M150は、取得可能コンテンツ一覧画面M100にて選択されたコンテンツの管理コンテンツ情報が表示される選択コンテンツ欄M151と「レンタル」項目と「購入」項目とからなる利用形態選択欄M152とから構成される。なお、図7において、反転表示されている利用形態は、現在、選択されている利用形態を示す。レンタルが反転表示されている場合には、利用形態として、「レンタル」が選択されており、逆に、購入が反転表示されている場合には、「購入」が選択されていることになる。

【0076】

利用者は、利用形態選択欄M152を用いて、コンテンツのレンタル又は、購入の選択を行うことができる。

【0077】

(C) レンタル用チケット選択画面情報

レンタル用チケット選択画面情報は、図8に一例として示すレンタル用チケット選択画面M200を生成するための情報である。レンタル用チケット選択画面M200は、取得可能コンテンツ一覧画面M100にて選択されたコンテンツのレンタルを行う場合に、使用するライセンスチケットを選択するために用いられる画面である。レンタル用チケット選択画面M200は、取得可能コンテンツ一覧画面M100にて選択されたコンテンツの管理コンテンツ情報が表示される選択コンテンツ欄M201と記録媒体100に記録されているライセンスチケットの中で、利用可能なライセンスチケットを表示する利用可能ライセンスチケット欄M202とから構成される。利用可能ライセンスチケット欄M202は、チケット番号と、利用可能コンテンツIDと、利用規則（レンタル）とからなるレンタル用ライセンスチケット情報を1個以上含んでいる。チケット番号は、利用可能なチケット番号を示す情報であり、利用可能コンテンツIDは、利用者が、コンテンツ提供装置400より、レンタル又は購入できるコンテンツIDであり、ライセンスチケットの利用可能コンテンツIDと同一のものである。また、利用規則（レンタル）は、レンタル期間を示す情報である。なお、図8において、反転表示されているレンタル用ライセンスチケット情報は、現在、選択されているレンタル用ライセンスチケット情報を示す。

【0078】

利用者は、利用可能ライセンスチケット欄M202を用いて、コンテンツのレンタル期間の選択を行うことができる。

【0079】

(D) 購入用チケット選択画面情報

購入用チケット選択画面情報は、図9に一例として示す購入用チケット選択画面M250を生成するための情報である。購入用チケット選択画面M250は、取得可能コンテンツ一覧画面M100にて選択されたコンテンツの購入を行う場合に、使用するライセンスチケットを選択するために用いられる画面である。購入用チケット選択画面M250は、取得可能コンテンツ一覧画面M100にて選択されたコンテンツの管理コンテンツ情報が表示される選択コンテンツ欄M251と記録媒体100に記録されているライセンスチケットの中で、利用可能なライセンスチケットを表示する利用可能ライセンスチケット欄M252とから構成される。利用可能ライセンスチケット欄M252は、チケット番号と、利用可能コンテンツIDと、利用規則（購入）とからなる購入用ライセンスチケット情報を1個以上含んでいる。チケット番号は、利用可能なチケット番号を示す情報であり、利用可能コンテンツIDは、利用者が、コンテンツ提供装置400より、レンタル又は購入できるコンテンツIDであり、ライセンスチケットの利用可能コンテンツIDと同一のものである。また、利用規則（購入）は、利用できる金額を示す情報である。なお、図9において、反転表示されている購入用ライセンスチケット情報は、現在、選択されている購入用ライセンスチケット情報を示す。ここで、コンテンツを購入する場合には、購入用ライセンスチケット情報を複数選択することができる。複数選択されている場合には、選択されている複数の購入用ライセンスチケット情報が反転表示されることになる。

【0080】

利用者は、利用可能ライセンスチケット欄M252を用いて、コンテンツの購入する際に使用するライセンスチケットの選択を行うことができる。

【0081】

(E) 配信要求プログラム

配信要求プログラムについて、図10及び図11に示す流れ図を用いて説明する。

【0082】

コンテンツ一覧情報を要求するコンテンツ一覧要求情報を生成し、生成したコンテンツ一覧要求情報を、再生装置200の第1入出力部を介してコンテンツ提供装置400へ送

信し（ステップS5）、コンテンツ提供装置400より、再生装置200の第1入出力部を介してコンテンツ一覧情報を受信する（ステップS10）。

【0083】

次に、取得可能コンテンツ一覧生成処理を行う（ステップS15）。さらに、選択コンテンツ受付処理を行い、配信を要求するコンテンツの管理コンテンツ情報を取得する（ステップS20）。

【0084】

取得した管理コンテンツ情報に含まれるコンテンツIDと利用状況テーブルT150とを用いて、配信を要求するコンテンツが、既にレンタル中であるか又は購入済であるか否かの判断を行う（ステップS25）。

【0085】

配信を要求するコンテンツが、既にレンタル中、又は購入済である場合には、取得不可を示す取得不可情報を生成し、生成した取得不可情報を出力し、動作を終了する（ステップS30）。

【0086】

配信を要求するコンテンツが、レンタル中ではなく、且つ未購入である場合には、取得した管理コンテンツ情報を一時的に記憶し、利用形態受付処理を行う（ステップS35）。

。

【0087】

次に、利用形態受付処理にて取得した利用形態が、レンタルであるか購入であるかの判断を行う（ステップS40）。

【0088】

利用形態が、レンタルである場合には、レンタル用使用チケット受付処理を行い、利用するレンタル用ライセンスチケット情報を取得する（ステップS45）。取得したレンタル用ライセンスチケット情報が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツに対して使用可能か否かを判断する（ステップS50）。つまり、取得した利用可能コンテンツIDがワイルドカードにて示されている場合には、その利用可能コンテンツIDの中で、数字が示されている部分が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツIDと一致するか否か、又は取得した利用可能コンテンツIDがワイルドカードを使用していない場合には、利用可能コンテンツIDに示されているコンテンツIDが、一時的に記憶している管理コンテンツ情報に含まれるコンテンツIDと一致するか否かを判断する。

【0089】

取得したレンタル用ライセンスチケット情報が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツに対して使用可能でないと判断する場合には、選択されたレンタル用ライセンスチケット情報が使用不可能であることを示すレンタル用ライセンスチケット使用不可情報を生成し、生成したレンタル用ライセンスチケット使用不可情報を出力し、動作を終了する（ステップS55）。

【0090】

取得したレンタル用ライセンスチケット情報が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツに対して使用可能であると判断する場合には、取得したレンタル用ライセンスチケット情報を一時的に記憶する（ステップS60）。

【0091】

利用形態が、購入である場合には、購入用使用チケット受付処理を行い、利用する購入用ライセンスチケット情報を取得する（ステップS65）。取得した購入用ライセンスチケット情報が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツに対して使用可能か否かを判断する（ステップS70）。つまり、取得した購入用ライセンスチケット情報に含まれる利用可能コンテンツIDがワイルドカードにて示されている場合には、その利用可能コンテンツIDの中で、数字が示されている部分が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツIDと一致するか否か、又は購入用ライセン

チケット情報に含まれる利用可能コンテンツIDがワイルドカードを使用していない場合には、利用可能コンテンツIDに示されているコンテンツIDが、一時的に記憶している管理コンテンツ情報に含まれるコンテンツIDと一致するか否かを判断する。

【0092】

取得した購入用ライセンスチケット情報が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツに対して使用可能でないと判断する場合には、選択された購入用ライセンスチケットが使用不可能であることを示す購入用ライセンスチケット使用不可情報を生成し、生成した購入用ライセンスチケット使用不可情報を出力し、動作を終了する（ステップS75）。

【0093】

取得した購入用ライセンスチケット情報が、一時的に記憶している管理コンテンツ情報に含まれるコンテンツに対して使用可能であると判断する場合には、さらに、取得した購入用ライセンスチケット情報と、一時的に記憶している管理コンテンツ情報とを用いて、取得した購入用ライセンスチケット情報に含まれる金額の合計が、取得した購入用ライセンスチケット情報に含まれる金額より不足しているか否かの判断を行う（ステップS80）。

【0094】

不足している場合には、購入不可を示す購入不可情報を生成し、生成した購入不可情報を出力し、動作を終了する（ステップS85）。不足していない場合には、取得した購入用ライセンスチケット情報を一時的に記憶する（ステップS90）。

【0095】

さらに、配信要求プログラムは、一時的に記憶している管理コンテンツ情報からコンテンツIDを取得し、取得したコンテンツIDを含むコンテンツ配信要求情報を生成し、生成したコンテンツ配信要求情報を再生装置200の第1入出力部を介してコンテンツ提供装置400へ送信する（ステップS95）。

【0096】

配信要求プログラムは、コンテンツ提供装置400より、再生装置200の第1入出力部を介して配信コンテンツ情報を受信する（ステップS100）。また、配信コンテンツ情報の受信完了後、配信コンテンツ情報の受信が完了した日時を示す受信完了日時を取得し、一時的に記憶する（ステップS105）。ここで、配信コンテンツ情報とは、コンテンツID、暗号化コンテンツ鍵及び暗号化コンテンツとからなる情報である。

【0097】

次に、配信要求プログラムは、利用形態がレンタルであるか購入であるかの判断を行う（ステップS110）。

【0098】

利用形態が、購入であると判断する場合には、購入処理を行い（ステップS115）、さらに、利用状況更新処理を行う（ステップS125）。

【0099】

利用形態が、レンタルであると判断する場合には、受信した配信コンテンツ情報を用いて、コンテンツIDと、暗号化コンテンツ鍵と暗号化コンテンツとからなる組とを対応付けて、レンタルコンテンツ記憶部131へ格納し（ステップS120）、利用状況更新処理を行う（ステップS125）。

【0100】

(F) 取得可能コンテンツ一覧生成処理

ここでは、配信要求プログラム内の取得可能コンテンツ一覧生成処理（図10におけるS15の処理）について、図12に示す流れ図を用いて説明する。

【0101】

ライセンスチケットテーブルT100と利用状況テーブルT150とを用いて、利用状態が未利用である全てのライセンスチケットより、利用可能コンテンツIDに記録されている各コンテンツIDを取得する（ステップS150）。

【0102】

取得した利用可能コンテンツIDに記録されている各コンテンツIDと、受信したコンテンツ一覧情報に含まれるコンテンツIDとを用いて、ライセンスチケットにて、レンタル又は購入可能なコンテンツの管理コンテンツ情報を抽出し、抽出した管理コンテンツ情報を用いて、取得可能コンテンツ一覧情報を生成する（ステップS155）。

【0103】

なお、ステップS155において、同ステップを取得した利用可能コンテンツIDの数分繰り返し、且つ既に抽出されている管理コンテンツ情報は抽出しないようにする。これにより、未利用であるライセンスチケットにて、レンタル又は購入可能なコンテンツに係る管理コンテンツ情報からなる取得可能コンテンツ一覧情報を生成することができる。

【0104】

(G) 選択コンテンツ受付処理

ここでは、配信要求プログラム内の選択コンテンツ受付処理（図10におけるS20の処理）について、図13に示す流れ図を用いて説明する。

【0105】

選択コンテンツ受付処理は、取得可能コンテンツ一覧生成処理にて生成された取得可能コンテンツ一覧情報を取得可能コンテンツ一覧画面M100とを用いて、再生装置200の出力部を介して接続されたテレビへ出力する（ステップS180）。

【0106】

次に、利用者より再生装置200が有するリモコンから情報を受け付け（ステップS185）、受け付けた情報が、コンテンツの選択が完了する旨を示すコンテンツ選択完了情報であるか否かの判断を行う（ステップS190）。コンテンツ選択完了情報であると判断する場合には、その時点で、反転表示されている管理コンテンツ情報を取得し、選択コンテンツ受付処理を終了する（ステップS195）。

【0107】

コンテンツ選択完了情報でないと判断する場合には、受け付けた情報が、現在反転表示されている情報から、1つ上の情報を反転表示するよう変更の旨を示す上方向変更情報であるか否かの判断を行う（ステップS200）。上方向変更情報であると判断する場合には、反転表示を行う管理コンテンツ情報を、現在の管理コンテンツ情報から、1つ上の管理コンテンツ情報へ変更し（ステップS205）、ステップS185へ戻る。例えば、図6に示す取得可能コンテンツ一覧画面M100において、上方向変更情報を受け取ると、配信要求処理部203は、反転表示を管理コンテンツ情報M102から、管理コンテンツ情報M101へ変更する。

【0108】

上方向変更情報でないと判断する場合には、受け付けた情報が、現在反転表示されている情報から、1つ下の情報を反転表示するよう変更の旨を示す下方向変更情報であるか否かの判断を行う（ステップS210）。下方向変更情報であると判断する場合には、反転表示を行う管理コンテンツ情報を、現在の管理コンテンツ情報から、1つ下の管理コンテンツ情報へ変更し（ステップS215）、ステップS185へ戻る。例えば、図6に示す取得可能コンテンツ一覧画面M100において、下方向変更情報を受け取ると、配信要求処理部203は、反転表示を管理コンテンツ情報M102から、管理コンテンツ情報M103へ変更する。

【0109】

下方向変更情報でないと判断する場合には、受け付けた情報が、現在表示されているページから次ページの取得可能コンテンツ一覧を表示するよう変更の旨を示す次ページ変更情報であるか否かの判断を行う（ステップS220）。次ページ変更情報であると判断する場合には、次ページの取得可能コンテンツ一覧を表示し（ステップS225）、ステップS185へ戻る。

【0110】

次ページ変更情報でないと判断する場合には、受け付けた情報が、現在表示されている

ページから前ページの取得可能コンテンツ一覧を表示するよう変更の旨を示す前ページ変更情報であるか否かの判断を行う（ステップS230）。前ページ変更情報であると判断する場合には、ページの取得可能コンテンツ一覧を表示し（ステップS235）、ステップS185へ戻る。

【0111】

前ページ変更情報でないと判断する場合には、ステップS185へ戻る。

【0112】

(H) 利用形態受付処理

ここでは、配信要求プログラム内の利用形態受付処理（図10におけるS35の処理）について、図14に示す流れ図を用いて説明する。

【0113】

利用形態受付処理は、選択コンテンツ受付処理にて取得した管理コンテンツ情報を利用形態選択画面M150とを用いて、再生装置200の出力部を介して接続されたテレビへ出力する（ステップS250）。

【0114】

次に、利用者より情報を受け付け（ステップS255）、受け付けた情報が、利用形態の選択が完了する旨を示す利用形態選択完了情報であるか否かの判断を行う（ステップS260）。利用形態選択完了情報であると判断する場合には、その時点で、反転表示されている利用形態を取得し、利用形態受付処理を終了する（ステップS265）。

【0115】

利用形態選択完了情報でないと判断する場合には、受け付けた情報が、上方向変更情報であるか否かの判断を行う（ステップS270）。上方向変更情報であると判断する場合には、反転表示を行う利用形態を、1つ上の利用形態へと変更し（ステップS275）、ステップS255へ戻る。

【0116】

上方向変更情報でないと判断する場合には、受け付けた情報が、下方向変更情報であるか否かの判断を行う（ステップS280）。下方向変更情報であると判断する場合には、現在反転表示されている利用形態から、1つ下の利用形態へと変更し（ステップS285）、ステップS255へ戻る。

【0117】

下方向変更情報でないと判断する場合には、ステップS255へ戻る。

【0118】

(I) レンタル用使用チケット受付処理

ここでは、配信要求プログラム内のレンタル用使用チケット受付処理（図10におけるS45の処理）について、図15に示す流れ図を用いて説明する。

【0119】

レンタル用使用チケット受付処理は、記録媒体100のライセンスチケットテーブルT100と利用状況テーブルT150とを用いて、「未利用」であるライセンスチケットを全て取得する（ステップS300）。さらに、取得したライセンスチケットと、一時的に記憶している管理コンテンツ情報を、レンタル用チケット選択画面M200を用いて、再生装置200の出力部を介して接続されたテレビへ出力する（ステップS305）。

【0120】

次に、利用者より情報を受け付け（ステップS310）、受け付けた情報が、レンタル用ライセンスチケット情報の選択の完了を示すレンタル用チケット選択完了情報であるか否かの判断を行う（ステップS315）。

【0121】

レンタル用チケット選択完了情報であると判断する場合には、その時点で、反転表示されているレンタル用ライセンスチケット情報を取得し、レンタル用使用チケット受付処理を終了する（ステップS320）。

【0122】

レンタル用チケット選択完了情報でないと判断する場合には、受け付けた情報が、上方方向変更情報であるか否かの判断を行う（ステップS325）。上方方向変更情報であると判断する場合には、反転表示を行うレンタル用ライセンスチケット情報を、1つ上のレンタル用ライセンスチケット情報へと変更し（ステップS330）、ステップS310へ戻る。

【0123】

上方方向変更情報でないと判断する場合には、受け付けた情報が、下方向変更情報であるか否かの判断を行う（ステップS335）。下方向変更情報であると判断する場合には、現在反転表示されているレンタル用ライセンスチケット情報から、1つ下のレンタル用ライセンスチケット情報へと変更し（ステップS340）、ステップS310へ戻る。

【0124】

下方向変更情報でないと判断する場合には、ステップS310へ戻る。

【0125】

（J） 購入用使用チケット受付処理

ここでは、配信要求プログラム内の購入用使用チケット受付処理（図10におけるS65の処理）について、図16に示す流れ図を用いて説明する。

【0126】

購入用使用チケット受付処理は、記録媒体100のライセンスチケットテーブルT100と利用状況テーブルT150とを用いて、「未利用」であるライセンスチケットを全て取得する（ステップS350）。さらに、取得したライセンスチケットと、一時的に記憶している管理コンテンツ情報を、購入用チケット選択画面M250を用いて、出力部206を介して、再生装置200と接続されたテレビへ出力する（ステップS355）。

【0127】

次に、利用者より情報を受け付け（ステップS360）、受け付けた情報が、購入用ライセンスチケット情報の選択の完了を示す購入用チケット選択完了情報であるか否かの判断を行う（ステップS365）。購入用チケット選択完了情報であると判断する場合には、その時点で、反転表示されている購入用ライセンスチケット情報を取得し、購入用使用チケット受付処理を終了する（ステップS370）。

【0128】

購入用チケット選択完了情報でないと判断する場合には、受け付けた情報が、ライセンスチケットを複数利用することを示す複数利用情報であるか否かの判断を行う（ステップS375）。複数利用情報であると判断する場合には、現在反転表示されている購入用ライセンスチケット情報を、購入用ライセンスチケット情報の選択の完了を示す購入用チケット選択完了情報を受信するまで、反転表示のままとなるように反転表示を固定し（ステップS380）、ステップS360へ戻る。

【0129】

複数利用情報でないと判断する場合には、上方方向変更情報であるか否かの判断を行う（ステップS385）。上方方向変更情報であると判断する場合には、反転表示を行う購入用ライセンスチケット情報を、1つ上のレンタル用ライセンスチケット情報へと変更し（ステップS390）、ステップS360へ戻る。

【0130】

なお、上方方向変更情報を受信する前に、複数利用情報を受信している場合には、現在反転表示されている購入用ライセンスチケット情報は反転表示に固定されているため、現在反転表示されている購入用ライセンスチケット情報は反転表示されたままで、1つ上の購入用ライセンスチケット情報の反転表示を行うこととなる。複数利用情報を受信していない場合には、現在反転表示されている購入用ライセンスチケット情報は通常の表示に変更し、1つ上の購入用ライセンスチケット情報の反転表示を行うこととなる。

【0131】

上方方向変更情報でないと判断する場合には、受け付けた情報が、下方向変更情報であるか否かの判断を行う（ステップS395）。下方向変更情報であると判断する場合には、

現在反転表示されているレンタル用ライセンスチケット情報から、1つ下のレンタル用ライセンスチケット情報へと変更し（ステップS400）、ステップS360へ戻る。

【0132】

なお、下方向変更情報を受信する前に、複数利用情報を受信している場合には、現在反転表示されている購入用ライセンスチケット情報は反転表示に固定されているため、現在反転表示されている購入用ライセンスチケット情報は反転表示されたままで、1つ下の購入用ライセンスチケット情報の反転表示を行うこととなる。複数利用情報を受信していない場合には、現在反転表示されている購入用ライセンスチケット情報は通常の表示に変更し、1つ下の購入用ライセンスチケット情報の反転表示を行うこととなる。

【0133】

下方向変更情報でないと判断する場合には、ステップS360へ戻る。

【0134】

(K) 購入処理

ここでは、配信要求プログラム内の購入処理（図11におけるS115の処理）について、図17に示す流れ図を用いて説明する。

【0135】

購入用使用チケット受付処理にて、取得した購入用ライセンスチケット情報を用いて、購入用ライセンスチケット情報に対応するライセンスチケットに含まれるチケット用暗号化マスタ鍵を取得する（ステップS420）。このとき、購入用ライセンスチケット情報を複数記憶している場合には、各購入用ライセンスチケット情報に対応するライセンスチケットの中で、チケット番号が最小であるライセンスチケットより、チケット用暗号化マスタ鍵を取得する。

【0136】

次に、購入処理は、再生装置200が有するデバイス鍵を取得して、取得したチケット用暗号化マスタ鍵を復号して、マスタ鍵を生成する（ステップS425）。次に、生成したマスタ鍵を用いて、受信した配信コンテンツ情報に含まれる暗号化コンテンツ鍵を復号して、コンテンツ鍵を生成し（ステップS430）、さらに、生成したコンテンツ鍵を用いて、受信した配信コンテンツ情報に含まれる暗号化コンテンツを復号して、コンテンツを生成する（ステップS435）。生成したコンテンツを購入コンテンツ記憶部132へ格納する（ステップS440）。

【0137】

(L) 利用状況更新処理

ここでは、配信要求プログラム内の利用状況更新処理（図11におけるS125の処理）について、図18に示す流れ図を用いて説明する。

【0138】

利用状況更新処理は、利用形態がレンタルであるか否かの判断を行う（ステップS450）。

【0139】

レンタルであると判断する場合には、一時的に記憶しているレンタル用ライセンスチケット情報に含まれるチケット番号と対応するライセンスチケット利用情報を取得する（ステップS455）。このとき、取得したライセンスチケット利用情報に含まれる利用状態は、「未利用」であり、利用形態、利用開始日時、コンテンツID、コンテンツ名及び定価には、何も記録されていない状態である。

【0140】

次に、取得したライセンスチケット利用情報の利用状態を「利用中」と変更し、利用形態を「レンタル」とし、さらに、一時的に記憶しているレンタル用ライセンスチケット情報と配信コンテンツ情報の受信完了日時とを用いて、利用開始日時、コンテンツID、コンテンツ名及び定価へ各情報を書き込み、利用状況テーブルT100の更新を行う（ステップS460）。

【0141】

レンタルでないと判断する場合には、一時的に記憶している購入用ライセンスチケット情報に含まれるチケット番号と対応するライセンスチケット利用情報を取得する（ステップS465）。このとき、購入用ライセンスチケットが複数記憶されている場合には、各購入用ライセンスチケット情報に含まれるチケット番号と対応する全てのライセンスチケット利用情報を取得する。また、このとき、取得したライセンスチケット利用情報に含まれる利用状態は、「未利用」であり、利用形態、利用開始日時、コンテンツID、コンテンツ名及び定価には、何も記録されていない状態である。

【0142】

配信要求処理部203は、取得したライセンスチケット利用情報の利用状態を「利用済」と変更し、利用形態を「購入」とし、さらに、一時的に記憶している購入用ライセンスチケット情報と配信コンテンツ情報の受信完了日時とを用いて、利用開始日時、コンテンツID、コンテンツ名及び定価へ各情報を書き込み、利用状況テーブルT100の更新を行う（ステップS470）。なお、一時的に記憶している購入用ライセンスチケット情報の数分繰り返す。

【0143】

1. 3 再生装置200の構成

ここでは、再生装置200の構成について説明する。再生装置200は、コンテンツ提供装置400に対してデータの送受信、記録媒体100に対してデータの入出力及び、記録媒体100に記憶されているコンテンツの再生を行う装置である。

【0144】

再生装置200は、図19に示すように、デバイス鍵記憶部201、時計部202、配信要求処理部203、再生処理部204、入力部205、出力部206、第1入出力部207、第2入出力部208及びリモコン210とから構成されている。

【0145】

再生装置200は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置200は、その機能を達成する。

【0146】

また、再生装置200は、図示していないが、出力部206を用いて、テレビと接続されている。なお、再生装置200と接続されるものは、テレビに限定はされない。再生装置200より出力される映像、音声、又は双方を出力できる装置であればよい。

【0147】

なお、第1サブシステム11、12が有する再生装置は、再生装置200と同様の構成を有しているため、説明は省略する。

【0148】

また、以降において、コンテンツ鍵を「CK」、コンテンツを「CNT」として説明を行う。

【0149】

1. 3. 1 デバイス鍵記憶部201

デバイス鍵記憶部201は、チケット用暗号化マスタ鍵を復号するためのデバイス鍵「DK」を記憶している。

【0150】

デバイス鍵とは、コンテンツの再生を許可された装置のみが持つ鍵である。

【0151】

1. 3. 2 時計部202

時計部202は、年月日及び時刻の計時を行う。

【0152】

1. 3. 3 配信要求処理部203

配信要求処理部203は、再生装置200に記録媒体100が装着され、且つ再生装置200がコンテンツ提供装置400とインターネットを介してネットワーク接続されている状態で、コンテンツ提供装置400へコンテンツの配信要求及び受信を行う。

【0153】

配信要求処理部203は、リモコン210より入力部205を介して、コンテンツ配信要求の開始を示す配信要求開始指示情報を受け取る。配信要求処理部203は、配信要求開始指示情報を受け取ると、記録媒体100の配信要求機能記憶部120より第2入出力部208を介して、取得可能コンテンツ一覧画面情報、利用形態選択画面情報、レンタル用チケット選択画面情報、購入用チケット選択画面情報、及び配信要求プログラムを読み出し、読み出した配信要求プログラムを実行する。

【0154】

1. 3. 4 再生処理部204

再生処理部204は、再生装置200に記録媒体100が装着されている状態で、コンテンツの再生を行う。再生処理部204は、再生可能コンテンツ一覧画面情報を予め記憶している。

【0155】

再生可能コンテンツ一覧画面情報は、図20に一例として示す再生可能コンテンツ一覧画面M300を生成するための情報である。再生可能コンテンツ一覧画面M300は、再生装置200にて、再生可能なコンテンツを表示ために用いられる画面である。再生可能コンテンツ一覧画面M300は、記録媒体100に記録されているコンテンツの中で、再生可能なコンテンツを表示する再生可能コンテンツ欄M301から構成される。再生可能コンテンツ欄M301は、利用番号とコンテンツIDとコンテンツ名とからなる再生可能コンテンツ情報を1個以上含んでいる。

【0156】

利用番号は、ライセンスチケット利用情報に割り当てられている番号であり、ライセンスチケットのチケット番号と対応している。コンテンツIDは、各コンテンツに付加された識別子であり、コンテンツ名は、コンテンツIDと対応するコンテンツの名称である。なお、図20において、反転表示されている再生可能コンテンツ情報は、現在、選択されている再生可能コンテンツ情報を示す。利用者は、取得可能コンテンツ一覧画面M100より、レンタル又は購入したいコンテンツの選択を行うことができる。

【0157】

なお、図20の再生可能コンテンツ一覧画面M300では、再生可能コンテンツ情報を2件表示しているが、取得可能コンテンツ一覧画面M100と同様に、5件毎の表示にしてもよい。また、表示される再生可能コンテンツ情報が6件以上存在する場合には、現在表示されているページから次ページへの切り替え又は前ページの切り替えを行う。

【0158】

再生処理部204は、リモコン210より入力部205を介して、コンテンツ再生の開始を示す再生開始指示情報を受け取る。再生処理部204は、再生開始指示情報を受け取ると、以下の動作を行う。

【0159】

先ず、時計部202より、現在の日時を取得する。次に、利用状況テーブルT150よりライセンスチケット利用情報を取得する。取得したライセンスチケット利用情報に含まれる利用状態が「利用中」であるか否かを判断する。「利用中」であると判断する場合には、取得したライセンスチケット利用情報に含まれる利用開始日時と、時計部202より取得した日時とを用いて、利用開始日時からの経過時間を算出し、算出した経過時間と、取得したライセンスチケット利用情報と対応するライセンスチケットに含まれるレンタルの日数とを用いて、経過時間がレンタルの日数内であるか否かの判断を行う。レンタル日数内でないと判断する場合には、取得したライセンスチケット利用情報の利用状態を「利用済」に変更し、ライセンスチケット利用情報の更新を行う。この動作を利用状況テーブルT150に含まれるライセンスチケット利用情報の数分繰り返すことにより、利用状況

テーブルT150全体の更新がされる。

【0160】

次に、更新された利用状況テーブルT150より、利用状態が「利用中」であるライセンスチケット利用情報、又は利用状態が「利用済」且つ利用形態が「購入」であるライセンスチケット利用情報の取得を行い、取得したライセンスチケット利用情報を一時的に記憶する。なお、利用状態が「利用済」且つ利用形態が「購入」であるライセンスチケット利用情報の取得の際に、同一のコンテンツIDが複数存在する場合には、取得したライセンスチケット利用情報のうち利用番号が最小であるライセンスチケット利用情報を一時的に記憶する。

【0161】

取得したライセンスチケット利用情報より、再生可能コンテンツ情報を生成し、生成した再生可能コンテンツ情報を再生可能コンテンツ一覧画面M300を用いて、出力部206を介して、再生装置200と接続されたテレビへ出力する。

【0162】

再生処理部204は、上方向変更情報をリモコン210より入力部205を介して、受信すると、現在反転表示されている再生可能コンテンツ情報を、1つ上の再生可能コンテンツ情報の反転表示を行い、下方向変更情報をリモコン210より入力部205を介して、受信すると、現在反転表示されている再生可能コンテンツ情報を、1つ下の再生可能コンテンツ情報の反転表示を行う。

【0163】

再生処理部204は、リモコン210より、再生可能コンテンツ情報を選択の完了を示す再生可能コンテンツ選択完了情報を受け取ると、その時点で、反転表示されている再生可能コンテンツ情報を取得し、さらに、一時的に記憶しているライセンスチケット利用情報の中で、取得した再生可能コンテンツ情報の利用番号と一致するライセンスチケット利用情報を取得する。取得したライセンスチケット利用情報の利用形態が、レンタルであるか購入であるかの判断を行う。

【0164】

購入である場合には、購入コンテンツ記憶部132より、取得したライセンスチケット利用情報のコンテンツIDに対応するコンテンツ「CNT」の再生を行う。

【0165】

レンタルである場合には、レンタルコンテンツ記憶部131より、取得したライセンスチケット利用情報に含まれるコンテンツIDに対応する暗号化コンテンツ鍵と暗号化コンテンツとの組を取得する。さらに、取得したライセンスチケット利用情報の利用番号と対応するライセンスチケットに含まれるチケット用暗号化マスタ鍵E_{nc} (DK, WK) を取得する。再生処理部204は、再生装置200が有するデバイス鍵「DK」を用いて、取得したチケット用暗号化マスタ鍵E_{nc} (DK, WK) を復号し、次に、復号したマスター鍵「WK」を用いて、取得した暗号化コンテンツ鍵E_{nc} (WK, CK) を復号し、さらに、復号して得られたコンテンツ鍵「CK」を用いて、取得した暗号化コンテンツE_{nc} (CK, CNT) の復号を行い、復号して得られたコンテンツ「CNT」の再生を行う。再生終了後、復号して得られたコンテンツ「CNT」を消去する。

【0166】

1. 3. 5 入力部205

入力部205は、リモコン210より送信された情報を受信し、配信要求処理部203又は再生処理部204へ出力する。

【0167】

1. 3. 6 出力部206

出力部206は、配信要求処理部203より受け取った情報又は再生処理部204より受け取った情報を、接続されたテレビへ出力する。

【0168】

1. 3. 7 第1入出力部207

第1出入力部207は、配信要求処理部203より受け取った情報をインターネットを介して、コンテンツ提供装置400へ送信する。また、コンテンツ提供装置400よりインターネットを介して受信した情報を配信要求処理部203へ出力する。

【0169】

1. 3. 8 第2出入力部208

第2出入力部208は、記録媒体100から読み出した情報を配信要求処理部203又は再生処理部204へ出力する。

【0170】

また、配信要求処理部203又は再生処理部204から受け取った情報を記録媒体100へ出力する。

【0171】

1. 3. 9 リモコン210

リモコン210は、利用者のキー操作により、受け取った情報を入力部205へ出力する。

【0172】

1. 4 ライセンスチケット生成装置300の構成

ここでは、ライセンスチケット生成装置300の構成について説明する。ライセンスチケット生成装置300は、ライセンスチケットを生成し、生成したライセンスチケットを記録媒体へ書き込む装置である。

【0173】

ライセンスチケット生成装置300は、図21に示すデバイス鍵記憶部301、暗号鍵記憶部302、マスタ鍵生成部303、チケット用暗号化部304、ライセンスチケット生成部305、書込部306、出力用暗号化部307、出力部308及びチケット情報記憶部309とから構成されている。

【0174】

ライセンスチケット生成装置300は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モデムなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ライセンスチケット生成装置300は、その機能を達成する。

【0175】

ライセンスチケット生成装置300は、マスタ鍵を生成し、生成したマスタ鍵を用いて、ライセンスチケットを生成する。さらに、生成したライセンスチケットを記録媒体に書き込む。また、生成したライセンスチケットを記録媒体に書き込む動作を繰り返すことにより、ライセンスチケットが書き込まれた記録媒体の大量生産を行う。

【0176】

1. 4. 1 デバイス鍵記憶部301

デバイス鍵記憶部301は、マスタ鍵を共通鍵暗号により暗号化するためのデバイス鍵を記憶している。

【0177】

なお、デバイス鍵記憶部301が記憶しているデバイス鍵と、再生装置200にて記憶しているデバイス鍵は、同一の鍵である。

【0178】

1. 4. 2 暗号鍵記憶部302

暗号鍵記憶部302は、マスタ鍵生成部303にて生成されたマスタ鍵を共通鍵暗号により暗号化するための暗号鍵「K」を記憶している。

【0179】

1. 4. 3 マスタ鍵生成部303

マスタ鍵生成部303は、乱数を用いて、マスタ鍵「WK」を生成し、生成したマスタ

鍵「WK」をチケット用暗号化部304と出力用暗号化部307とへ出力する。

【0180】

1. 4. 4 チケット情報記憶部309

チケット情報記憶部309は、ライセンスチケット生成部305により生成されたライセンスチケットテーブルT100及び利用状況テーブルT150を記憶する領域を備えている。

【0181】

チケット情報記憶部309にて記憶されているライセンスチケットテーブルT100及び利用状況テーブルT150が記録媒体100へ書き込まれることになる。なお、利用状況テーブルT150を形成するライセンスチケット利用情報は、利用番号と利用状態に「未利用」が記録されており、他の項目は空白である。

【0182】

また、チケット情報記憶部309は、配信要求機能を予め記憶している。

【0183】

1. 4. 5 チケット用暗号化部304

チケット用暗号化部304は、デバイス鍵記憶部301にて記憶されているデバイス鍵「DK」を用いて、マスタ鍵生成部303より受け取ったマスタ鍵「WK」を共通鍵暗号で、暗号化することにより、チケット用暗号化マスタ鍵E_{nc} (DK, WK)を生成し、生成したチケット用暗号化マスタ鍵E_{nc} (DK, WK)を記憶する。

【0184】

1. 4. 6 ライセンスチケット生成部305

ライセンスチケット生成部305は、利用可能コンテンツIDとして記録するコンテンツID及び、レンタルと購入との組からなる利用規則を予め記憶している。

【0185】

ライセンスチケット生成部305は、チケット用暗号化部304にて記憶されているチケット用暗号化マスタ鍵E_{nc} (DK, WK)と、予め記憶している利用可能コンテンツIDとして記録するコンテンツID及び利用規則とを用いて、ライセンスチケットテーブルT100を生成し、生成したライセンスチケットテーブルT100をチケット情報記憶部309へ格納する。

【0186】

さらに、利用状況テーブルT150をも生成し、生成した利用状況テーブルT150をチケット情報記憶部309へ格納する。

【0187】

1. 4. 7 書込部306

書込部306は、チケット情報記憶部309にて記憶されているライセンスチケットテーブルT100と、利用状況テーブルT150と、配信要求機能とを記録媒体100へ書き込む。

【0188】

ここで、ライセンスチケットテーブルT100、利用状況テーブルT150、配信要求機能をプレス加工にて、記録媒体100への書き込むことにより、低コストにて生産が可能となる。

【0189】

1. 4. 8 出力用暗号化部307

出力用暗号化部307は、暗号鍵記憶部302にて記憶されている暗号鍵「K」を用いて、マスタ鍵生成部303より受け取ったマスタ鍵「WK」を共通鍵暗号で、暗号化することにより、提供者用暗号化マスタ鍵E_{nc} (K, WK)を生成し、生成した提供者用暗号化マスタ鍵E_{nc} (K, WK)を出力部308を介してコンテンツ提供装置400へ送信する。

【0190】

1. 4. 9 出力部308

出力部308は、出力用暗号化部307より受け取った情報をコンテンツ提供装置400へ送信する。

【0191】

1. 5 コンテンツ提供装置400の構成

ここでは、コンテンツ提供装置400の構成について説明する。コンテンツ提供装置400は、再生装置200に対してデータの送受信及び、コンテンツの暗号化を行う装置である。

【0192】

コンテンツ提供装置400は、図22に示す復号鍵記憶部401、マスタ鍵記憶部402、コンテンツ関連情報記憶部403、配信データ記憶部404、受信部405、復号部406、入力部407、コンテンツ鍵生成部408、暗号化部409、コンテンツ読込部410、配信処理部411及び送受信部412とから構成されている。

【0193】

コンテンツ提供装置400は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モデムなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、コンテンツ提供装置400は、その機能を達成する。

【0194】

なお、コンテンツ提供装置400は、コンテンツIDと、コンテンツとからなるコンテンツ媒体の着脱が可能であり、コンテンツの暗号化を行う場合には、コンテンツ媒体が装着された状態で行う。

【0195】

1. 5. 1 復号鍵記憶部401

復号鍵記憶部401は、ライセンスチケット生成装置300にて生成された提供者用マスタ鍵を復号するための復号鍵を記憶している。

【0196】

1. 5. 2 マスタ鍵記憶部402

マスタ鍵記憶部402は、復号部406にて復号されたマスタ鍵を記憶する領域を備えている。

【0197】

1. 5. 3 コンテンツ関連情報記憶部403

コンテンツ関連情報記憶部403は、図23に一例として示すコンテンツ関連情報テーブルT400を有している。

【0198】

コンテンツ関連情報テーブルT400は、コンテンツID、コンテンツ名及び定価からなる組を1個以上記憶するための領域を備えている。

【0199】

コンテンツIDは、コンテンツごとに付加された識別子であり、コンテンツ名は、コンテンツの名称であり、定価は、コンテンツを購入する場合の値段である。

【0200】

1. 5. 4 配信データ記憶部404

配信データ記憶部404は、図24に一例として示す暗号化コンテンツ管理テーブルT410を有している。

【0201】

暗号化コンテンツ管理テーブルT410は、コンテンツID、コンテンツ名、暗号化コンテンツ鍵、暗号化コンテンツ鍵及び定価からなる組を1個以上記憶するための領域を備えている。

【0202】

コンテンツIDは、各コンテンツに付加されている識別子であり、コンテンツ名は、コンテンツの名称であり、暗号化コンテンツ鍵は、マスタ鍵にて暗号化されたコンテンツ鍵のデータであり、暗号化コンテンツは、コンテンツ鍵にて暗号化されたコンテンツのデータであり、定価は、コンテンツを購入する場合の値段である。

【0203】

なお、記録媒体100の構成において説明したように、「CNTn」(nは数字)は、コンテンツを示し、「CKn」(nは数字)は、コンテンツ鍵を示しており、異なるコンテンツに対して、異なるコンテンツ鍵が割り当てられている。

【0204】

1. 5. 5 受信部405

受信部405は、ライセンスチケット生成装置300より、提供者用暗号化マスタ鍵Enc(K, WK)を受信し、受信した提供者用暗号化マスタ鍵Enc(K, WK)を復号部406へ出力する。

【0205】

1. 5. 6 復号部406

復号部406は、受信部405より提供者用暗号化マスタ鍵Enc(K, WK)を受け取ると、復号鍵記憶部401より復号鍵を取得し、取得した復号鍵を用いて、提供者用暗号化マスタ鍵Enc(K, WK)の復号を行い、復号されたマスタ鍵「WK」をマスタ鍵記憶部402へ書き込む。

【0206】

1. 5. 7 入力部407

入力部407は、コンテンツの暗号化を開始する旨を示す暗号化開始情報を受け付け、受け付けた暗号化開始情報をコンテンツ鍵生成部408へ出力する。

【0207】

1. 5. 8 コンテンツ鍵生成部408

コンテンツ鍵生成部408は、入力部407より暗号化開始情報を受け取ると、乱数を用いて、コンテンツ鍵「CK」を生成し、生成したコンテンツ鍵「CK」を暗号化部409へ出力する。

【0208】

なお、コンテンツ鍵生成部408は、暗号化開始情報を受け付ける度に、異なるコンテンツ鍵を生成する。

【0209】

1. 5. 9 暗号化部409

暗号化部409は、コンテンツ鍵生成部408よりコンテンツ鍵「CK」を受け取ると、コンテンツID及びコンテンツのデータである「CNT」を取得する旨を示すコンテンツ取得開始情報をコンテンツ読込部410へ出力し、コンテンツ読込部410よりコンテンツIDとコンテンツ「CNT」を受け取る。

【0210】

さらに、受け取ったコンテンツ鍵「CK」を用いて、コンテンツ「CNT」を共通鍵暗号で暗号化することにより、暗号化コンテンツEnc(K, CNT)を生成する。

【0211】

暗号化部409は、マスタ鍵記憶部402よりマスタ鍵「WK」を取得し、取得したマスタ鍵「WK」を用いて、コンテンツ鍵「CK」を共通鍵暗号で、暗号化することにより、暗号化コンテンツ鍵Enc(WK, CK)を生成する。

【0212】

また、暗号化部409は、コンテンツ関連情報テーブルT400より、コンテンツ読込部410より受け取ったコンテンツIDに対応するコンテンツ名及び定価を取得する。

【0213】

暗号化部409は、生成した暗号化コンテンツEnc(K, CNT)と暗号化コンテンツ鍵Enc(WK, CK)とコンテンツ読込部410より受け取ったコンテンツIDと

、コンテンツ関連情報テーブルT400より取得したコンテンツ名及び定価とからなる組を配信データ記憶部404へ書き込む。

【0214】

1. 5. 10 コンテンツ読込部410

コンテンツ読込部410は、暗号化部409よりコンテンツ取得開始情報を受け取ると、装着されているコンテンツ媒体よりコンテンツID及びコンテンツのデータ「CNT」を取得し、取得したコンテンツID及びコンテンツのデータ「CNT」を暗号化部409へ出力する。

【0215】

1. 5. 11 配信処理部411

配信処理部411は、送受信部412を介して再生装置200よりコンテンツ一覧要求情報を受信すると、暗号化コンテンツ管理テーブルT410を用いて、コンテンツ一覧情報を作成し、再生装置200へ送受信部412を介して送信する。

【0216】

配信処理部411は、送受信部412を介して再生装置200よりコンテンツ配信要求情報を受信すると、暗号化コンテンツ管理テーブルT410より、受信したコンテンツ配信要求情報に含まれるコンテンツIDと一致するコンテンツID、暗号化コンテンツ鍵及び暗号化コンテンツを取得し、取得したコンテンツID、暗号化コンテンツ鍵及び暗号化コンテンツを用いて、配信コンテンツ情報を生成し、生成した配信コンテンツ情報を再生装置200へ送受信部412を介して送信する。

【0217】

1. 5. 12 送受信部412

送受信部412は、再生装置200よりインターネットを介して受信した情報を配信処理部411へ出力する。

【0218】

また、送受信部412は、情報を配信処理部411より受け取った情報をインターネットを介して再生装置200へ送信する。

【0219】

1. 6 プリペイドカードシステム1の動作

ここでは、プリペイドカードシステム1の動作について説明する。

【0220】

1. 6. 1 ライセンスチケット生成時の動作概要

ここでは、ライセンスチケット生成時の動作概要について、図25に示す流れ図を用いて、説明する。

【0221】

ライセンスチケット生成装置300は、ライセンスチケットの生成処理を行い、このときに生成された提供者用暗号化マスタ鍵E_nc (K、WK) をコンテンツ提供装置400へ送信する(ステップS500)。

【0222】

コンテンツ提供装置400は、ライセンスチケット生成装置300より提供者用暗号化マスタ鍵E_nc (K、WK) を受信し(ステップS505)、復号鍵記憶部401にて記憶している復号鍵を用いて、提供者用暗号化マスタ鍵E_nc (K、WK) を復号し、復号したマスタ鍵「WK」をマスタ鍵記憶部402へ書き込む(ステップS510)。

【0223】

1. 6. 2 コンテンツ配信要求時の動作概要

ここでは、コンテンツ配信要求時の動作概要について、図26に示す流れ図を用いて、説明する。なお、再生装置200は、記録媒体100が装着され、且つコンテンツ提供装置400とネットワーク接続されている状態である。

【0224】

再生装置200は、配信要求開始指示情報を受け取ると、記録媒体100より配信要求

機能を読み出し、配信要求機能を実行する（ステップS550）。次に、再生装置200は、コンテンツ提供装置400へコンテンツ一覧要求情報を送信する（ステップS555）。

【0225】

コンテンツ提供装置400は、再生装置200よりコンテンツ一覧要求情報を受信すると、コンテンツ一覧情報を生成し、生成したコンテンツ一覧情報を再生装置200へ送信する（ステップS560）。

【0226】

再生装置200は、コンテンツ提供装置400よりコンテンツ一覧情報を受信すると、受信したコンテンツ一覧情報とライセンスチケットテーブルT100を用いて、取得可能コンテンツ一覧情報を生成し、生成した取得可能コンテンツ一覧情報を用いて、利用者から取得するコンテンツの選択を受け付け、受け付けたコンテンツに係るコンテンツ配信要求情報を生成し、生成したコンテンツ配信要求情報をコンテンツ提供装置400へ送信する（ステップS565）。

【0227】

コンテンツ提供装置400は、再生装置200よりコンテンツ配信要求情報を受信すると、受信したコンテンツ配信要求情報を用いて、配信する暗号化コンテンツ、暗号化コンテンツ鍵及びコンテンツIDを取得し、取得した暗号化コンテンツ、暗号化コンテンツ鍵及びコンテンツIDを用いて、配信コンテンツ情報を生成し、生成した配信コンテンツ情報を再生装置200へ送信する（ステップS570）。

【0228】

再生装置200は、コンテンツ提供装置400より配信コンテンツ情報を受信すると、利用形態が、レンタルの場合には、受信した配信コンテンツ情報を、利用形態に応じた処理を行い、利用状況テーブルT150の更新を行う（ステップS575）。

【0229】

ここで、利用形態に応じた処理とは、以下に示す処理のことである。利用形態が、レンタルである場合には、受信した配信コンテンツ情報を用いて、コンテンツIDと、暗号化コンテンツ鍵と暗号化コンテンツとからなる組とを対応付けて、記録媒体100のレンタルコンテンツ記憶部131へ記憶し、利用形態が、購入である場合には、暗号化コンテンツを復号し、復号したコンテンツを記録媒体100の購入コンテンツ記憶部132へ記憶する。

【0230】

1. 6. 3 ライセンスチケット生成処理の動作

ここでは、ライセンスチケット生成装置300にて行われるライセンスチケット生成処理について、図27に示す流れ図を用いて、説明する。

【0231】

ライセンスチケット生成装置300は、マスタ鍵「WK」を生成し（ステップS600）、生成したマスタ鍵「WK」を、暗号鍵「K」を用いて共通鍵暗号で暗号化し、提供者用暗号化マスタ鍵E_{nc}（K、WK）を生成する（ステップS605）。生成した提供者用暗号化マスタ鍵E_{nc}（K、WK）をコンテンツ提供装置400へ送信する（ステップS610）。

【0232】

また、生成したマスタ鍵「WK」を、デバイス鍵「DK」を用いて共通鍵暗号で暗号化し、チケット用暗号化マスタ鍵E_{nc}（DK、WK）を生成し（ステップS615）、生成したチケット用暗号化マスタ鍵E_{nc}（DK、WK）と、記憶しているコンテンツID及び利用規則とを用いて、1以上のライセンスチケットからなるライセンスチケットテーブルT100を生成し、生成したライセンスチケットテーブルT100をチケット情報記憶部309へ格納する（ステップS620）。さらに、ライセンス利用状況情報を記憶部309へ格納する（ステップS625）。

【0233】

チケット情報記憶部309にて記憶しているライセンスチケットテーブルT100及び利用状況テーブルT150と、予め記憶している配信要求機能とを記録媒体100へ書き込む（ステップS630）。

【0234】

なお、ステップS630のみを繰り返すことで、記録媒体を複数生成することができる。

【0235】

1. 6. 4 コンテンツ取得処理の動作

ここでは、再生装置200において、コンテンツ取得時に行われるコンテンツ取得処理について、図28に示す流れ図を用いて、説明する。

【0236】

再生装置200は、取得開始情報を受け付け（ステップS650）、記録媒体100より配信要求プログラム、取得可能コンテンツ一覧画面情報、利用形態選択画面情報、レンタル用チケット選択画面情報、及び購入用チケット選択画面情報を読み出し（ステップS655）、配信要求プログラムを実行する（ステップS660）。

【0237】

1. 6. 5 再生処理の動作

ここでは、再生装置200にて行われる再生処理について、図29に示す流れ図を用いて、説明する。なお、ここでは、暗号化コンテンツをE nc (CK, CNT) し、暗号化コンテンツ鍵をE nc (WK, CK) とする。

【0238】

再生装置200は、再生開始指示情報を受け付ける（ステップS800）。次に、日時を取得し、利用状況テーブルT150の更新を行う（ステップS810）。

【0239】

更新された利用状況テーブルT150より、利用状態が「利用中」であるライセンスチケット利用情報、又は利用状態が「利用済」且つ利用形態が「購入」であるライセンスチケット利用情報の取得を行い、取得したライセンスチケット利用情報より再生可能コンテンツ情報を生成する（ステップS820）。生成した再生可能コンテンツ情報を出力し（ステップS830）、再生するコンテンツに係る再生可能コンテンツ情報の選択を受け付け（ステップS840）、ステップS820にて取得したライセンスチケット利用情報を用いて、受け付けた再生可能コンテンツが、レンタルであるか否かの判断を行う（ステップS850）。

【0240】

レンタルである場合には、取得したライセンスチケット利用情報含まれる利用番号に対応するライセンスチケットをライセンスチケットテーブルT100より取得し、取得したライセンスチケットに含まれるチケット用暗号化マスタ鍵E nc (DK, WK) を取得する（ステップS860）。

【0241】

取得したチケット用暗号化マスタ鍵E nc (DK, WK) を、記憶しているデバイス鍵「DK」を用いて、復号し、マスタ鍵「WK」を取得する（ステップS870）。

【0242】

また、受け付けた再生可能コンテンツ情報の含まれるコンテンツIDに対応する暗号化コンテンツ鍵E nc (WK, CK) と暗号化コンテンツE cn (CK, CNT) からなる組を、レンタルコンテンツ記憶部131より取得する（ステップS880）。

【0243】

ステップS870にて取得したマスタ鍵「WK」を用いて、取得した暗号化コンテンツ鍵E nc (WK, CK) を復号し、コンテンツ鍵「CK」を取得する（ステップS890）。取得したコンテンツ鍵「CK」を用いて、暗号化コンテンツE nc (CK, CNT) を復号する（ステップS900）。復号したコンテンツを再生する（ステップS910）。

。なお、再生が終了すると、復号されたコンテンツは消去される。

【0244】

ステップS850にて、レンタルでないと判断する場合には、受け付けた再生可能コンテンツ情報の含まれるコンテンツIDに対応するコンテンツを購入コンテンツ記憶部132より取得し、取得したコンテンツを再生する（ステップS920）。

【0245】

1. 6. 6 利用状態確認処理の動作

ここでは、再生処理時のステップS810にて行われる利用状態確認処理について、図30に示す流れ図を用いて、説明する。

【0246】

先ず、時計部202より、日時を取得する（ステップS1000）。

【0247】

次に、以下の処理を、利用状況テーブルT150内にあるライセンスチケット利用情報の数回繰り返す（ステップS1010）。

【0248】

ライセンスチケット利用情報を取得し（ステップS1020）、取得したライセンスチケット利用情報に含まれる利用状態が利用中であるか否かの判断を行う（ステップS1030）。

【0249】

利用中であると判断する場合には、取得した日時と、取得したライセンスチケット利用情報に含まれる利用開始日時とを用いて、経過時間を算出し（ステップS1040）、算出した経過時間が、取得したライセンスチケット利用情報と対応するライセンスチケットに含まれるレンタルの日数内であるか否かを判断する（ステップS1050）。利用中でない場合には、ステップS1020へ戻り、動作を繰り返す。

【0250】

レンタルの日数内ではない場合には、取得したライセンスチケット利用情報に含まれる利用状態を利用済に更新する（ステップS1060）。レンタルの日数内である場合には、ステップS1020へ戻り、動作を繰り返す。

【0251】

上記動作を、ライセンスチケット利用情報の数回繰り返し後、処理を終了する。

【0252】

1. 6. 7 暗号化コンテンツ生成処理の動作

ここでは、コンテンツ提供装置400にて行われるコンテンツの暗号化の動作について、図31に示す流れ図を用いて、説明する。

【0253】

コンテンツ提供装置400は、暗号化開始情報を受け付けると（ステップS1100）、コンテンツ鍵を生成する（ステップS1110）。

【0254】

次に、コンテンツ提供装置400に装着されたコンテンツ媒体より、コンテンツID及びコンテンツのデータを読み出す（ステップS1120）。読み出されたコンテンツのデータを、ステップS1010にて生成したコンテンツ鍵を用いて共通鍵暗号で暗号化し、暗号化コンテンツを生成する（ステップS1130）。

【0255】

次に、マスタ鍵記憶部402よりマスタ鍵を取得し（ステップS1140）、取得したマスタ鍵を用いて、コンテンツ鍵を共通鍵暗号で暗号化し、暗号化コンテンツ鍵を生成する（ステップS1150）。

【0256】

次に、コンテンツ関連情報記憶部403より、ステップS1120にて取得したコンテンツIDに対応するコンテンツ名及び定価をコンテンツ関連情報記憶部403より取得し、取得したコンテンツ名及び定価と、ステップS1120にて取得したコンテンツIDと

、生成した暗号化コンテンツ及び暗号化コンテンツ鍵とからなる組を、暗号化コンテンツ管理テーブルT410へ書き込む（ステップS1160）。

【0257】

1. 7 第1の実施の形態のまとめ

以上、説明したようにプリペイドカードシステム1においては、記録媒体100にてマスタ鍵が暗号化された暗号化マスタ鍵を記憶しており、コンテンツ提供装置400にてコンテンツ毎に、暗号化コンテンツ鍵及び暗号化コンテンツを暗号化コンテンツ管理テーブルを用いて記憶している。コンテンツ毎に生成された暗号化コンテンツ鍵は、記録媒体100に記憶している暗号化マスタ鍵を復号して、取得したマスタ鍵を用いて復号することが可能である。これは、利用者がコンテンツ提供装置400に対して配信要求できるコンテンツを限定しないことを意味している。つまり、利用者は、記録媒体100の購入時に購入するコンテンツを決定しておく必要がなく、記録媒体100の購入後、自由にコンテンツを選ぶことが可能となる。

【0258】

また、記録媒体100に、利用規則として期間を記憶しておくことにより、利用者は、記憶されている期間を指定して、コンテンツを入手した場合には、指定した期間内において、入手したコンテンツを視聴することができる。

【0259】

また、記録媒体100に入手可能なコンテンツIDとして、ワイルドカード表記を含めたコンテンツIDを記憶しておくことにより、利用者は、記憶されているワイルドカード表記を含めたコンテンツIDを用いて、コンテンツ提供装置400にて有している多数のコンテンツより、入手可能なコンテンツを抽出し、抽出した結果より、コンテンツを自由に選ぶことができる。

【0260】

また、記録媒体100の購入時に、コンテンツのレンタル又は購入に関する料金を支払っているため、インターネットを用いた決済方法を実現するためのPKIや、利用者の利用料金を管理するセンタを必要としない。そのため、煩雑な処理を行う必要がないため、簡単な仕組みでシステムを構成することができる。また、他の決済方法として、キオスク端末にて、購入コンテンツを記録媒体にて記録し販売する決済方法があるが、この場合には、購入コンテンツは予め決めておく必要がある。しかしながら、上記に記述したように、記録媒体の購入時には、購入するコンテンツを決めておく必要がないため、キオスク端末において利用される決済方法を用いる必要がない。

【0261】

また、コンテンツ鍵を暗号化するために用いるマスタ鍵を、コンテンツの再生が可能な再生装置が持つデバイス鍵を用いて、共通鍵暗号で暗号化を行うことにより、コンテンツの再生が不可能な装置にて、マスタ鍵を読みとて暴露するのを防止することができる。

【0262】

2. 第2の実施の形態

2. 1 プリペイドカードシステム2の構成

本発明に係る第2の実施の形態としてのプリペイドカードシステム2について、説明する。プリペイドカードシステム2の構成は、第1の実施の形態で示したプリペイドカードシステム1の構成と同様であり、図32に示す第1サブシステム10A、11A、…、12A及び第2サブシステム20Aとから構成される。第1サブシステム10Aは、記録媒体100Aと、記録媒体100Aの着脱が可能な再生装置200Aとから構成される。ここで、記録媒体100Aは、光ディスクである。なお、第1サブシステム11A、…、12Aは、第1サブシステム10Aと同様の構成である。第2サブシステム20Aは、ライセンスチケット生成装置300Aとコンテンツ提供装置400Aとから構成され、ライセンスチケット生成装置300Aとコンテンツ提供装置400Aとは、専用線を用いてネットワーク接続されている。

【0263】

プリペイドカードシステム2において、暗号化コンテンツ鍵を生成する場合に、Broadcast Encryption(以下、「BE」という。)を用いる点がプリペイドカードシステム1と異なる点である。

【0264】

ここで、BEについて、簡単に説明する。BEとは、再生機器毎に異なるデバイス鍵を与えておき、再生を許可しない再生機器のデバイス鍵では、復号できないようにする暗号化方法である。つまり、再生を許可しない再生機器のデバイス鍵を用いて暗号化された暗号化マスタ鍵の送信を行わないことで、再生を許可しない再生機器のデバイス鍵では、復号できなくなる。

【0265】

本実施の形態では、デバイス鍵ではなくマスタ鍵を用いてBEを適用する。

【0266】

以下に、マスタ鍵を用いたBEについて、簡単に説明する。各ライセンスチケットに含まれる暗号化マスタ鍵をそれぞれ異なる暗号化マスタ鍵とする。つまり、各マスタ鍵はそれぞれ異なっている。また、コンテンツ提供装置400Aは、暗号化コンテンツの生成と、各マスタ鍵を用いて、複数の暗号化コンテンツ鍵の生成とを行う。コンテンツ提供装置400Aは、配信要求に基いて、配信コンテンツ情報を送信し、再生装置200Aは、配信コンテンツ情報を受信する。ここで、配信コンテンツ情報は、コンテンツIDと、暗号化コンテンツと、複数の暗号化コンテンツ鍵及び暗号化コンテンツ鍵を復号に使用できるマスタ鍵に係る情報を示すインデックス情報を組とからなる情報である。インデックス情報は、1つの暗号化コンテンツ鍵に対して、1つ生成され、当該暗号化コンテンツ鍵と対応付けられている。ここで、インデックス情報には、ライセンスチケットのチケット番号を使用する。ライセンスチケットのチケット番号を用いることで、暗号化マスタ鍵を復号して取得したマスタ鍵と、そのマスタ鍵で復号できる暗号化コンテンツ鍵との対応付けが可能となる。

【0267】

これにより、あるマスタ鍵が暴露された場合には、暴露されたマスタ鍵にて生成された暗号化コンテンツ鍵及びインデックス情報を、配信コンテンツ情報から除くことにより、再生装置200Aでは、暴露されたマスタ鍵では、暗号化コンテンツ鍵の復号ができないため、コンテンツの再生が不可能となる。

【0268】

以降では、プリペイドカードシステム1と異なる点を中心に説明する。

【0269】

2.2 記録媒体100Aの構成

ここでは、記録媒体100Aの構成について説明する。

【0270】

記録媒体100Aは、図33に示すROM領域101AとRAM領域102Aとから構成されている。ROM領域101Aは、読み出しのみが可能な領域であり、ライセンスチケット記憶部110Aと配信要求機能記憶部120Aとを有している。RAM領域102Aは、読み出し及び書き込みが可能な領域であり、コンテンツ記憶部130Aと利用状況記憶部140Aとを有している。

【0271】

なお、第1サブシステム11A、…、12Aが有する記録媒体は、記録媒体100と同様の構成を有しているため、説明は省略する。

【0272】

2.2.1 ライセンスチケット記憶部110A

ライセンスチケット記憶部110Aは、図34に一例として示すように、ライセンスチケットテーブルT100Aを有している。

【0273】

ライセンスチケットテーブルT100Aにおけるデータ構造の構成は、第1の実施の形

態で示したライセンスチケットテーブルT100と同様であるため、説明は省略する。

【0274】

第1の実施の形態と異なる点は、ライセンスチケット毎に記録される暗号化マスタ鍵が、全て異なる暗号化マスタ鍵であるという点である。

【0275】

2. 2. 2 配信要求機能記憶部120A

配信要求機能記憶部120Aは、第1の実施の形態で示した配信要求機能記憶部120と同様に取得可能コンテンツ一覧画面情報、利用形態選択画面情報、レンタル用チケット選択画面情報、購入用チケット選択画面情報、及び配信要求プログラムを記憶している。

【0276】

ここで、第1の実施の形態で示した配信要求プログラムとは、購入処理における動作がことなる。ここでは、その異なる点について、第1の実施の形態で示した図17を用いて、説明する。

【0277】

購入処理は、ステップS420及びS425の実行後、コンテンツ提供装置400Aより受信した配信コンテンツ情報に含まれるインデックス情報と、一時的に記憶している購入用ライセンスチケット情報に含まれるチケット番号とを用いて、インデックス情報と一致するチケット番号のライセンスチケットに含まれるチケット用暗号化マスタ鍵を取得するステップを追加する。

【0278】

このステップの実行後、図17に示すステップS430以降を実行する。

【0279】

2. 2. 3 コンテンツ記憶部130A

コンテンツ記憶部130Aは、第1の実施の形態で示したコンテンツ記憶部130と同様の構成であるが、レンタルコンテンツ記憶部131Aにて、暗号化コンテンツの記憶方法のみが、第1の実施の形態と異なる。図35に示すように、レンタルコンテンツ記憶部131Aは、インデックス情報と暗号化コンテンツ鍵からなる組と、暗号化コンテンツとをコンテンツIDと対応付けて記憶している。ここで、インデックス情報と暗号化コンテンツ鍵との組からなる数は、再生が許可されているマスタ鍵の数となる。

【0280】

2. 2. 4 利用状況記憶部140A

利用状況記憶部140Aは、第1の実施の形態で示した利用状況記憶部140と同様に利用状況テーブルT150Aを有している。利用状況テーブルT150Aのデータ構造は、利用状況テーブルT150と同様であるため、説明は省略する。

【0281】

2. 3 再生装置200Aの構成

ここでは、再生装置200Aの構成について説明する。

【0282】

再生装置200Aは、図36に示すように、デバイス鍵記憶部201A、時計部202A、配信要求処理部203A、再生処理部204A、入力部205A、出力部206A、第1入出力部207A、第2入出力部208A及びリモコン210Aとから構成されている。

【0283】

再生装置200Aは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置200Aは、その機能を達成する。

【0284】

また、再生装置200Aは、図示していないが、出力部206Aを用いて、テレビと接

続されている。なお、再生装置200Aと接続されるものは、テレビに限定はされない。再生装置200Aより出力される映像、音声、又は双方を出力できる装置であればよい。

【0285】

なお、第1サブシステム11A、・・・、12Aが有する再生装置は、再生装置200Aと同様の構成を有しているため、説明は省略する。

【0286】

2. 3. 1 デバイス鍵記憶部201A

デバイス鍵記憶部201Aは、第1の実施の形態で示したデバイス鍵記憶部201と同様であるため、説明は省略する。

【0287】

2. 3. 2 時計部202A

時計部202Aは、第1の実施の形態で示した時計部202と同様であるため、説明は省略する。

【0288】

2. 3. 3 配信要求処理部203A

配信要求処理部203Aは、リモコン210Aより入力部205Aを介して、コンテンツ配信要求の開始を示す配信要求開始指示情報を受け取る。配信要求処理部203Aは、配信要求開始指示情報を受け取ると、記録媒体100Aより第2入出力部208Aを介して、配信要求機能を読み出し、読み出した配信要求機能を実行する。以下、配信要求処理部203Aが実行する配信要求機能について、第1の実施の形態と異なる点を中心に詳細に説明する。

【0289】

異なる点は、購入時において、配信コンテンツ情報の受信後に行う暗号化コンテンツ鍵及び暗号化コンテンツ鍵の復号における動作が異なる。以下に、配信コンテンツ情報受信後の動作について説明する。

【0290】

配信要求処理部203Aは、コンテンツ提供装置400Aより、配信コンテンツ情報を受信する。また、配信コンテンツ情報の受信が完了後、受信完了日時を時計部202Aにより取得し、一時的に記憶する。次に、受信した配信コンテンツ情報に含まれるインデックス情報と、一時的に記憶している購入用ライセンスチケット情報に含まれるチケット番号とを用いて、インデックス情報と一致するチケット番号のライセンスチケットに含まれるチケット用暗号化マスタ鍵を取得する。

【0291】

配信要求処理部203Aは、再生装置200Aが有するデバイス鍵「DK」を用いて、取得したチケット用暗号化マスタ鍵を復号することにより、マスタ鍵を取得する。次に、復号に利用したライセンスチケットのチケット番号と一致するインデックス情報に対応付けられた暗号化コンテンツ鍵を取得する。取得した暗号化コンテンツ鍵に対して、取得したマスタ鍵を用いて、復号を行い、コンテンツ鍵「CK」を取得し、さらに、取得したコンテンツ鍵「CK」を用いて、受信した配信コンテンツ情報に含まれる暗号化コンテンツEnc(CK, CNT)を復号することにより、コンテンツ「CNT」を取得し、取得したコンテンツ「CNT」を記録媒体100Aの購入コンテンツ記憶部132へ格納する。

【0292】

配信要求処理部203Aは、一時的に記憶している購入用ライセンスチケット情報と、利用形態と、時計部202Aより取得した配信コンテンツ情報の受信完了日時を用いて、利用状況テーブルT150Aの更新を行う。更新方法は、第1の実施の形態で示した方法と同様であるため、説明は省略する。

【0293】

2. 3. 4 再生処理部204A

再生処理部204Aは、再生装置200Aに記録媒体100Aが装着されている状態で、コンテンツの再生を行う。

【0294】

再生処理部204Aは、第1の実施の形態で示した再生処理部204と同様であるため、説明は省略する。

【0295】

ただし、レンタルコンテンツを再生する場合に行われる暗号化コンテンツ鍵の取得では、ライセンスチケットのチケット番号と一致するインデックス情報と対応する暗号化コンテンツ鍵を取得し、取得した暗号化コンテンツ鍵を、復号して得たマスタ鍵を用いて、復号することとなる。

【0296】**2. 3. 5 入力部205A**

入力部205Aは、第1の実施の形態で示した入力部205と同様であるため、説明は省略する。

【0297】**2. 3. 6 出力部206A**

出力部206Aは、第1の実施の形態で示した出力部206と同様であるため、説明は省略する。

【0298】**2. 3. 7 第1入出力部207A**

第1入出力部207Aは、第1の実施の形態で示した第1入出力部207と同様であるため、説明は省略する。

【0299】**2. 3. 8 第2入出力部208A**

第2入出力部208Aは、第1の実施の形態で示した第2入出力部208と同様であるため、説明は省略する。

【0300】**2. 3. 9 リモコン210A**

リモコン210Aは、第1の実施の形態で示したリモコン210と同様であるため、説明は省略する。

【0301】**2. 4 ライセンスチケット生成装置300Aの構成**

ここでは、ライセンスチケット生成装置300Aの構成について説明する。

【0302】

ライセンスチケット生成装置300Aは、図37に示すデバイス鍵記憶部301A、暗号鍵記憶部302A、マスタ鍵生成部303A、チケット用暗号化部304A、ライセンスチケット生成部305A、書込部306A、出力用暗号化部307A、チケット情報記憶部309A、送受信部320A及びライセンスチケット変更部321Aとから構成されている。

【0303】

ライセンスチケット生成装置300Aは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モ뎀などから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ライセンスチケット生成装置300Aは、その機能を達成する。

【0304】

ライセンスチケット生成装置300Aは、複数のマスタ鍵を生成し、生成した複数マスタ鍵を用いて、各暗号化マスタ鍵の内容が異なるライセンスチケットを生成する。さらに、生成したライセンスチケットを記録媒体に書き込む。また、生成したライセンスチケットを記録媒体に書き込む動作を繰り返すことにより、ライセンスチケットが書き込まれた記録媒体の大量生産を行う。

【0305】

また、コンテンツ提供装置400Aより、コンテンツの復号には利用しないマスタ鍵を示すマスタ鍵無効化情報を受信し、受信したマスタ鍵無効化情報を用いて、ライセンスチケットの生成を行う。

【0306】

2. 4. 1 デバイス鍵記憶部301A

デバイス鍵記憶部301Aは、第1の実施の形態にて示したデバイス鍵記憶部301と同様であるため、説明は省略する。

【0307】

2. 4. 2 暗号鍵記憶部302A

暗号鍵記憶部302Aは、マスタ鍵生成部303Aにて生成された複数のマスタ鍵を共通鍵暗号により暗号化するための暗号鍵「K」を記憶している。

【0308】

2. 4. 3 マスタ鍵生成部303A

マスタ鍵生成部303Aは、乱数を用いて、マスタ鍵「WK1」、「WK2」、・・・、「WK10」を生成し、生成した各マスタ鍵をチケット用暗号化部304Aと出力用暗号化部307Aとへ出力する。なお、マスタ鍵「WK1」、「WK2」、・・・、「WK10」は、異なったマスタ鍵である。

【0309】

2. 4. 4 チケット情報記憶部309A

チケット情報記憶部309Aは、ライセンスチケットテーブルT100A及び利用状況テーブルT150Aを記憶する領域を備えている。

【0310】

チケット情報記憶部309Aにて記憶されているライセンスチケットテーブルT100A及び利用状況テーブルT150Aが記録媒体100Aへ書き込まれることになる。

【0311】

なお、利用状況テーブルT150Aのデータ構造は、第1の実施の形態にて示した利用状況テーブルT150のデータ構造と同様であるため、説明は省略する。また、利用状況テーブルT150Aを形成するライセンスチケット利用情報は、利用番号と利用状態に「未利用」が記録されており、他の項目は空白である。

【0312】

また、チケット情報記憶部309Aは、配信要求機能を予め記憶している。

【0313】

2. 4. 5 チケット用暗号化部304A

チケット用暗号化部304Aは、デバイス鍵記憶部301Aにて記憶されているデバイス鍵「DK」を用いて、マスタ鍵生成部303Aより受け取ったマスタ鍵「WK1」、「WK2」、・・・、「WK10」を共通鍵暗号で、それぞれ暗号化することにより、チケット用暗号化マスタ鍵E_{nc}(DK, WK1)、E_{nc}(DK, WK2)、・・・、E_{nc}(DK, WK10)を生成し、生成した各チケット用暗号化マスタ鍵を記憶する。

【0314】

2. 4. 6 ライセンスチケット生成部305A

ライセンスチケット生成部305Aは、利用可能コンテンツIDとして記録するコンテンツID及び、レンタルと購入との組からなる利用規則を予め記憶している。

【0315】

ライセンスチケット生成部305Aは、チケット用暗号化部304Aにて記憶されているチケット用暗号化マスタ鍵E_{nc}(DK, WK1)、E_{nc}(DK, WK2)、・・・、E_{nc}(DK, WK10)と、予め記憶している利用可能コンテンツIDとして記録するコンテンツID及び利用規則とを用いて、ライセンスチケットテーブルT100Aを生成し、生成したライセンスチケットテーブルT100Aをチケット情報記憶部309Aへ格納する。

【0316】

さらに、利用状況テーブルT150Aをも生成し、生成した利用状況テーブルT150Aをチケット情報記憶部309Aへ格納する。

【0317】

2. 4. 7 ライセンスチケット変更部321A

ライセンスチケット変更部321Aは、コンテンツ提供装置400Aより送受信部320Aを介して、マスタ鍵無効化情報を受信すると、チケット情報記憶部309Aにて記憶しているライセンスチケットテーブルT100Aより、受信したマスタ鍵無効化情報を用いて、利用できないマスタ鍵を含むライセンスチケットを削除して、ライセンスチケットテーブルT100Aを更新する。さらに、チケット情報記憶部309Aにて記憶している利用状況テーブルT150Aより、削除されたライセンスチケットに対応するライセンスチケット利用情報を削除して、利用状況テーブルT150Aを更新する。

【0318】

2. 4. 8 書込部306A

書込部306Aは、チケット情報記憶部309Aにて記憶しているライセンスチケットテーブルT100Aと、利用状況テーブルT150Aと、配信要求機能とを記録媒体100Aへ書き込む。

【0319】

ここで、ライセンスチケットテーブルT100A、利用状況テーブルT150A、配信要求機能をプレス加工にて、記録媒体100Aへの書き込むことにより、低コストにて生産が可能となる。

【0320】

2. 4. 9 出力用暗号化部307A

出力用暗号化部307Aは、暗号鍵記憶部302Aにて記憶されている暗号鍵「K」を用いて、マスタ鍵生成部303Aより受け取ったマスタ鍵「WK1」、「WK2」、…、「WK10」を共通鍵暗号で、それぞれ暗号化することにより、提供者用暗号化マスタ鍵E_{nc}(K, WK1)、E_{nc}(K, WK2)、…、E_{nc}(K, WK10)を生成し、生成した各提供者用暗号化マスタ鍵を送受信部320Aを介してコンテンツ提供装置400Aへ送信する。

【0321】

2. 4. 10 送受信部320A

送受信部320Aは、出力用暗号化部307Aより受け取った情報をコンテンツ提供装置400Bへ送信する。また、コンテンツ提供装置400Aより受信した情報をライセンスチケット生成部305Aへ出力する。

【0322】

2. 5 コンテンツ提供装置400Aの構成

ここでは、コンテンツ提供装置400Aの構成について説明する。

【0323】

コンテンツ提供装置400Aは、図38に示す復号鍵記憶部401A、マスタ鍵記憶部402A、コンテンツ関連情報記憶部403A、配信データ記憶部404A、復号部406A、入力部407A、コンテンツ鍵生成部408A、暗号化部409A、コンテンツ読込部410A、配信処理部411A、第1送受信部420A、第2送受信部421A及び無効化処理部422Aとから構成されている。

【0324】

コンテンツ提供装置400Aは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モデムなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、コンテンツ提供装置400Aは、その機能を達成する。

【0325】

なお、コンテンツ提供装置400Aは、コンテンツIDと、コンテンツとからなるコンテンツ媒体の着脱が可能であり、コンテンツの暗号化を行う場合には、コンテンツ媒体が装着された状態で行う。

【0326】

2.5.1 復号鍵記憶部401A

復号鍵記憶部401Aは、第1の実施の形態にて示した復号鍵記憶部401と同様であるため、説明は省略する。

【0327】

2.5.2 マスタ鍵記憶部402A

マスタ鍵記憶部402Aは、復号部406Aにて復号された複数のマスタ鍵を記憶する領域を備えている。

【0328】

2.5.3 コンテンツ関連情報記憶部403A

コンテンツ関連情報記憶部403Aは、第1の実施の形態で示したコンテンツ関連情報記憶部403と同様に、コンテンツ関連情報テーブルT400Aを有している。

【0329】

コンテンツ関連情報テーブルT400Aは、コンテンツ関連情報テーブルT400と同様であるため、説明は省略する。

【0330】

2.5.4 配信データ記憶部404A

配信データ記憶部404Aは、第1の実施の形態にて示した配信データ記憶部404と同様に、暗号化コンテンツ管理テーブルT410Aを有している。

【0331】

暗号化コンテンツ管理テーブルT410Aは、暗号化コンテンツ管理テーブルT410と同様であるため、説明は省略する。

【0332】

ここでは、暗号化コンテンツ管理テーブルT410Aを形成するコンテンツID、コンテンツ名、暗号化コンテンツ鍵、暗号化コンテンツ鍵及び定価からなる組を暗号化コンテンツ情報と呼ぶ。

【0333】

なお、暗号化コンテンツ情報に含まれる暗号化コンテンツ鍵には、インデックス情報とそれに対応する暗号化コンテンツ鍵との組が複数記憶されている。インデックス情報とそれに対応する暗号化コンテンツ鍵との組は、暗号化コンテンツ鍵を復号できるマスタ鍵の個数となる。

【0334】

2.5.5 第1送受信部420A

第1送受信部420Aは、ライセンスチケット生成装置300Aより、提供者用暗号化マスタ鍵Enc(K、WK1)、Enc(K、WK2)、…、Enc(K、WK10)を受信し、受信した提供者用暗号化マスタ鍵Enc(K、WK1)、Enc(K、WK2)、…、Enc(K、WK10)を復号部406Aへ出力する。

【0335】

また、無効化処理部422Aよりマスタ鍵無効化情報を受け取ると、受け取ったマスタ鍵無効化情報をライセンスチケット生成装置300Aへ送信する。

【0336】

2.5.6 復号部406A

復号部406Aは、第1送受信部420Aより提供者用暗号化マスタ鍵Enc(K、WK1)、Enc(K、WK2)、…、Enc(K、WK10)を受け取ると、復号鍵記憶部401Aより復号鍵を取得し、取得した復号鍵を用いて、提供者用暗号化マスタ鍵Enc(K、WK1)、Enc(K、WK2)、…、Enc(K、WK10)の復号

を行い、復号されたマスタ鍵「WK1」、「WK2」、・・・、「WK10」をマスタ鍵記憶部402Aへ書き込む。

【0337】

2. 5. 7 入力部407A

入力部407Aは、暗号化開始情報を受け付け、受け付けた暗号化開始情報をコンテンツ鍵生成部408Aへ出力する。

【0338】

また、マスタ鍵無効化情報を受け付け、受け付けたマスタ鍵無効化情報を無効化処理部422Aへ出力する。

【0339】

2. 5. 8 コンテンツ鍵生成部408A

コンテンツ鍵生成部408Aは、第1の実施の形態にて示したコンテンツ鍵生成部408と同様であるため、説明は省略する。

【0340】

2. 5. 9 無効化処理部422A

無効化処理部422Aは、各マスタ鍵とライセンスチケットのチケット番号との対応情報を予め記憶している。

【0341】

無効化処理部422Aは、入力部407Aより、マスタ鍵無効化情報を受け取ると、受け取ったマスタ鍵無効化情報を用いて、利用できないマスタ鍵をマスタ鍵記憶部402Aより削除し、マスタ鍵記憶部402Aの内容を更新する。また、受け取ったマスタ鍵無効化情報を用いて、暗号化コンテンツ管理テーブルT410Aの暗号化コンテンツ鍵より、無効化されたマスタ鍵にて暗号化された暗号化コンテンツ鍵及びそのインデックス情報を削除する。この動作を暗号化コンテンツ管理テーブルT410Aに記録されている全ての情報に対して行う。

【0342】

さらに、受け取ったマスタ鍵無効化情報を第1送受信部420Aを介してライセンスチケット生成装置300Aへ送信する。

【0343】

2. 5. 10 暗号化部409A

暗号化部409Aは、各マスタ鍵とライセンスチケットのチケット番号との対応情報を予め記憶している。

【0344】

暗号化部409Aは、コンテンツ鍵生成部408Aよりコンテンツ鍵「CK」を受け取ると、コンテンツID及びコンテンツのデータである「CNT」を取得する旨を示すコンテンツ取得開始情報をコンテンツ読込部410Aへ出力し、コンテンツ読込部410AよりコンテンツIDとコンテンツ「CNT」を受け取る。

【0345】

さらに、受け取ったコンテンツ鍵「CK」を用いて、コンテンツ「CNT」を共通鍵暗号で暗号化することにより、暗号化コンテンツEnc(CK, CNT)を生成する。

【0346】

暗号化部409Aは、マスタ鍵記憶部402Aよりマスタ鍵「WK1」、「WK2」、・・・、「WK10」を取得し、取得したマスタ鍵「WK1」、「WK2」、・・・、「WK10」を用いて、コンテンツ鍵「CK」を共通鍵暗号で、暗号化することにより、暗号化コンテンツ鍵Enc(WK1, CK)、Enc(WK2, CK)、・・・、Enc(WK10, CK)を生成する。さらに、生成した暗号化コンテンツ鍵Enc(WK1, CK)、Enc(WK2, CK)、・・・、Enc(WK10, CK)と、予め記憶している各マスタ鍵とライセンスチケットのチケット番号との対応情報を用いて、各コンテンツ鍵にインデックス情報を付加し、インデックス情報と暗号化コンテンツ鍵との組からなる情報(1, Enc(WK1, CK))、(2, Enc(WK2, CK))、・・・、(

10、E n c (WK10、CK) を生成する。

【0347】

また、暗号化部409Aは、コンテンツ関連情報テーブルT400Aより、コンテンツ読込部410Aより受け取ったコンテンツIDに対応するコンテンツ名及び定価を取得する。

【0348】

暗号化部409Aは、生成した暗号化コンテンツE n c (CK、CNT) と、インデックス情報と暗号化コンテンツ鍵との組からなる情報(1、E n c (WK1、CK))、(2、E n c (WK2、CK))、……、(10、E n c (WK10、CK))と、コンテンツ読込部410Aより受け取ったコンテンツIDと、コンテンツ関連情報テーブルT400Aより取得したコンテンツ名及び定価とからなる組を配信データ記憶部404Aへ書き込む。

【0349】

なお、無効化処理部422Aにて、マスタ鍵記憶部402Aの内容が更新されている場合には、その内容に基いて、暗号化コンテンツ鍵が生成される。例えば、無効化処理部422Aにて、利用できないマスタ鍵として「WK2」をマスタ鍵記憶部402Aより削除している場合には、暗号化コンテンツE n c (WK2、CK) は生成されない。つまり、マスタ鍵記憶部402Aにて記憶されているマスタ鍵のみを用いて、暗号化コンテンツ鍵を生成する。

【0350】

2. 5. 11 コンテンツ読込部410A

コンテンツ読込部410Aは、第1の実施の形態にて示したコンテンツ読込部410と同様であるため、説明は省略する。

【0351】

2. 5. 12 配信処理部411A

配信処理部411Aは、第2送受信部421Aを介して再生装置200Aよりコンテンツ一覧要求情報を受信すると、暗号化コンテンツ管理テーブルT410Aを用いて、コンテンツ一覧情報を生成し、再生装置200Aへ第2送受信部421Aを介して送信する。

【0352】

配信処理部411Aは、第2送受信部421Aを介して再生装置200Aよりコンテンツ配信要求情報を受信すると、暗号化コンテンツ管理テーブルT410Aより、受信したコンテンツ配信要求情報に含まれるコンテンツIDと一致するコンテンツID、1以上のインデックス情報と暗号化コンテンツ鍵との組、及び暗号化コンテンツを取得し、取得したコンテンツID、1以上のインデックス情報と暗号化コンテンツ鍵との組、及び暗号化コンテンツを用いて、配信コンテンツ情報を生成し、生成した配信コンテンツ情報を再生装置200Aへ第2送受信部421Aを介して送信する。

【0353】

2. 5.. 13 第2送受信部421A

第2送受信部421Aは、第1の実施の形態にて示した送受信部412と同様である為、説明は省略する。

【0354】

2. 6 プリペイドカードシステム2の動作

ここでは、プリペイドカードシステム2の動作について説明する。

【0355】

2. 6. 1 ライセンスチケット生成時の動作概要

ライセンスチケット生成時の動作概要は、第1の実施の形態において示した図25の流れ図と同様であるため、説明は省略する。

【0356】

ただし、ライセンスチケット生成装置300Aがコンテンツ提供装置400Aへ送信する提供者用暗号化マスタ鍵は、E n c (K、WK1)、E n c (K、WK2)、……、

Enc (K, WK10) である。また、コンテンツ提供装置400Aが、受信する提供者用暗号化マスタ鍵も同様に、Enc (K, WK1)、Enc (K, WK2)、…、Enc (K, WK10) であり、受信した提供者用暗号化マスタ鍵Enc (K, WK1)、Enc (K, WK2)、…、Enc (K, WK10) をそれぞれ復号することとなる。

【0357】

2. 6. 2 コンテンツ配信要求時の動作概要

コンテンツ配信要求時の動作概要は、第1の実施の形態において示した図26の流れ図と同様であるため、説明は省略する。

【0358】

2. 6. 3 ライセンスチケット生成処理の動作

ライセンスチケット生成装置300Aにて行われるライセンスチケット生成処理は、第1の実施の形態にて示した図27の流れ図と同様であるため、説明は省略する。

【0359】

ただし、ここで生成されるマスタ鍵は、「WK1」、「WK2」、…、「WK10」であり、さらに、ここで生成される提供者用暗号化マスタ鍵は、Enc (K, WK1)、Enc (K, WK2)、…、Enc (K, WK10) であり、これらの暗号化マスタ鍵がコンテンツ提供装置400Aへ送信される。さらに、生成されるチケット用暗号化マスタ鍵は、Enc (DK, WK1)、Enc (DK, WK2)、…、Enc (DK, WK10) であり、生成されたこれらのチケット用暗号化マスタ鍵を用いて、ライセンスチケットテーブルT100Aが生成される。

【0360】

2. 6. 4 ライセンスチケット変更処理の動作

ライセンスチケット生成装置300Aが、コンテンツ提供装置400Aよりマスタ鍵無効化情報を受信した際に行うライセンスチケット変更処理の動作について、図39に示す流れ図を用いて、説明する。

【0361】

ライセンスチケット生成装置300Aは、コンテンツ提供装置400Aよりマスタ鍵無効化情報を受信する（ステップS2000）。受信したマスタ鍵無効化情報を用いて、利用できないマスタ鍵に対応するライセンスチケットを、ライセンスチケットテーブルT100Aより削除し（ステップS2010）、さらに、削除したライセンスチケットに対応するライセンスチケット利用情報を、利用状況テーブルT150Aより削除する（ステップS2020）。

【0362】

これにより、チケット情報記憶部309Aの内容が更新される。なお、ライセンスチケット生成処理における書き込みステップのみを行うことで、更新された内容を記憶媒体に書き込むことが可能となる。

【0363】

2. 6. 5 コンテンツ取得処理の動作

再生装置200Aにおいて、コンテンツ取得時に行われるコンテンツ取得処理は、第1の実施の形態にて示した図28の流れ図と同様であるため、説明は省略する。

【0364】

2. 6. 6 再生処理の動作

再生装置200Aにて行われる再生処理は、第1の実施の形態にて示した図29の流れ図と同様であるため、説明は省略する。

【0365】

ただし、暗号化コンテンツ鍵を取得する際には、レンタルコンテンツを再生する場合に行われる暗号化コンテンツ鍵の取得では、ライセンスチケットのチケット番号と一致するインデックス情報を対応する暗号化コンテンツ鍵を取得する。

【0366】

2. 6. 7 利用状態確認処理の動作

再生処理時に行われる利用状態確認処理は、第1の実施の形態にて示した図30の流れ図と同様であるため、説明は省略する。

【0367】

2. 6. 8 暗号化コンテンツ生成処理の動作

コンテンツ提供装置400Aにて行われるコンテンツの暗号化の動作は、第1の実施の形態にて示した図31の流れ図と同様であるため、説明は省略する。

【0368】

ただし、生成される暗号化コンテンツ鍵の個数は、マスタ鍵記憶部402Aにて記憶しているマスタ鍵の個数であり、暗号化コンテンツ管理テーブルT410Aへ書き込まれる情報は、コンテンツIDと、生成した暗号化コンテンツと、暗号化コンテンツ鍵と、各暗号化コンテンツ鍵に対応するインデックス情報である。

【0369】

2. 6. 9 マスタ鍵無効化処理

コンテンツ提供装置400Aが、マスタ鍵無効化情報を受け取った場合に行うマスタ鍵無効化について、図40に示す流れ図を用いて、説明する。

【0370】

コンテンツ提供装置400は、マスタ鍵無効化情報を受け取ると（ステップS2100）、受け取ったマスタ鍵無効化情報を用いて、利用できないマスタ鍵をマスタ鍵記憶部402Aより削除し、マスタ鍵記憶部402Aの内容を更新する（ステップS2110）。次に、受け取ったマスタ鍵無効化情報を用いて、暗号化コンテンツ管理テーブルT410Aの暗号化コンテンツ鍵より、無効化されたマスタ鍵にて暗号化された暗号化コンテンツ鍵及びそのインデックス情報を削除する（ステップS2120）。

【0371】

さらに、受け取ったマスタ鍵無効化情報をライセンスチケット生成装置300Aへ送信する（ステップS2130）。

【0372】

なお、ステップS2120は、暗号化コンテンツ管理テーブルT410Aに記録されている全ての情報に対して行う。

【0373】

2. 7 第2の実施の形態のまとめ

以上、説明したようにプリペイドカードシステム2においては、記録媒体100Aにてマスタ鍵が暗号化された暗号化マスタ鍵を記憶しており、コンテンツ提供装置400Aにてコンテンツ毎に、暗号化コンテンツ鍵及び暗号化コンテンツを暗号化コンテンツ管理テーブルを用いて記憶している。コンテンツ毎に生成された暗号化コンテンツ鍵は、記録媒体100Aに記憶している暗号化マスタ鍵を復号して、取得したマスタ鍵を用いて復号することが可能である。これは、利用者がコンテンツ提供装置400Aに対して配信要求できるコンテンツを限定しないことを意味している。つまり、利用者は、記録媒体100Aの購入時に購入するコンテンツを決定しておく必要がなく、記録媒体100Aの購入後、自由にコンテンツを選ぶことが可能となる。

【0374】

また、記録媒体100Aに、利用規則として期間を記憶しておくことにより、利用者は、記憶されている期間を指定して、コンテンツを入手した場合には、指定した期間内において、入手したコンテンツを視聴することができる。

【0375】

また、記録媒体100Aに入手可能なコンテンツIDとして、ワイルドカード表記を含めたコンテンツIDを記憶しておくことにより、利用者は、記憶されているワイルドカード表記を含めたコンテンツIDを用いて、コンテンツ提供装置400Aにて有している多数のコンテンツより、入手可能なコンテンツを抽出し、抽出した結果より、コンテンツを自由に選ぶことができる。

【0376】

また、記録媒体100Aの購入時に、コンテンツのレンタル又は購入に関する料金を支払っているため、インターネットを用いた決済方法を実現するためのPKIや、料金を管理するセンタを必要としない。そのため、煩雑な処理を行う必要がないため、簡単な仕組みでシステムを構成することができる。また、他の決済方法として、キオスク端末にて、購入コンテンツを記録媒体にて記録し販売する決済方法があるが、この場合には、購入コンテンツは予め決めておく必要がある。しかしながら、上記に記述したように、記録媒体の購入時には、購入するコンテンツを決めておく必要がないため、キオスク端末において利用される決済方法を用いる必要がない。

【0377】

また、コンテンツ鍵を暗号化するために用いるマスタ鍵を、コンテンツの再生が可能な再生装置が持つデバイス鍵を用いて、共通鍵暗号で暗号化を行うことにより、コンテンツの再生が不可能な装置にて、マスタ鍵を読みとて暴露するのを防止することができる。

【0378】

また、暗号化コンテンツ鍵の暗号化方法にBEを用いていることにより、万一、マスタ鍵が暴露された場合には、その暴露されたマスタ鍵を無効化することにより、コンテンツを復号できないようにすることができ、セキュリティが向上される。

【0379】

3. 第3の実施の形態

3.1 プリペイドカードシステム3の構成

本発明に係る第2の実施の形態としてのプリペイドカードシステム3について、説明する。プリペイドカードシステム3の構成は、第2の実施の形態で示したプリペイドカードシステム2の構成と同様であり、図41に示す第1サブシステム10B、11B、...、12B及び第2サブシステム20Bとから構成される。第1サブシステム10Bは、記録媒体100Bと、記録媒体100Bの着脱が可能な再生装置200Bとから構成される。ここで、記録媒体100Bは、光ディスクである。なお、第1サブシステム11B、...、12Bは、第1サブシステム10Bと同様の構成である。第2サブシステム20Bは、ライセンスチケット生成装置300Bとコンテンツ提供装置400Bとから構成され、ライセンスチケット生成装置300Bとコンテンツ提供装置400Bとは、専用線を用いてネットワーク接続されている。

【0380】

プリペイドカードシステム3は、プリペイドカードシステム2とマスタ鍵の管理方法及びBEの適用方法が異なる。

【0381】

本実施の形態では、マスタ鍵の管理を木構造にて管理する。ここで用いる鍵管理方式は、中野稔久他著による「デジタルコンテンツ保護用鍵管理方式—木構造パターン分割方式—」（暗号と情報セキュリティシンポジウム2002）にて、提案された木構造パターン分割方式である。

【0382】

なお、木構造パターン分割方式では、デバイス鍵を用いているが、ここでは、デバイス鍵に替わりにマスタ鍵を用いる。

【0383】

図42を用いて、マスタ鍵を用いた木構造パターン分割方式による鍵管理について、説明する。

【0384】

ここで、図42に示す「A」、「B」、「C」、「D」、「E」、「F」、「G」は、ノードと呼ばれ、特に最上位層にあるノード「A」は、ルートと呼ばれ、最下位層にあるノード「D」、「E」、「F」、「G」は、リーフと呼ばれる。また、ノード間を連結することをパスによる連結という。また、木構造におけるノードの位置する各層をレイヤと呼び、上位から0、1、2の順に番号を付加したものをレイヤ番号（以下、「LN」とい

う。)と呼ぶ。例えば、ノード「A」のレイヤ番号は、「0」であり、ノード「B」、「C」のレイヤ番号は、「1」であり、ノード「D」、「E」、「F」、「G」のレイヤ番号は、「2」である。また、あるノードから上に伸びる1つのパスにより連結されているノードをそのノードの親ノードと呼ぶ。例えば、ノード「B」の親ノードは、ノード「A」となる。また、あるノードから下に派生した複数のパスにより連結されているノードをそのノードの子ノードと呼ぶ。例えば、ノード「B」の子ノードは、ノード「D」、「E」となる。また、各レイヤには複数のノードが存在するため、それらを識別する識別番号を木構造の左から0、1、…の順に付与する。これを相対ノード番号(以下、「RNN」という。)と呼ぶ。また、あるノードの子孫に、無効化されるべきリーフが存在する場合、そのノードを無効化ノードと呼ぶ。例えば、リーフ「E」が無効化される場合には、無効化ノードは、ノード「A」、「B」となる。また、あるノードの子ノードが無効化ノードであるか否かを、「0」、「1」にて表記する。無効化ノードでない場合を「0」、無効化ノードである場合を「1」とする。さらに、それらの値を木構造の左から結合したものをノード無効化パターン(以下、「NRP」という。)と呼ぶ。例えば、ノード「A」のNRPは、「00」、「10」、「01」の3パターンとなる。

【0385】

マスタ鍵を用いた木構造パターン分割方式による鍵管理では、リーフを除く各ノードに、NRPのパターン毎に、互いに異なるマスタ鍵を割り当てる。割り当てられたマスタ鍵には、それぞれを識別するための情報として、LN、RNN、NRPを付与する。LN、RNN、NRPが付与されたマスタ鍵を「LN-RNN-KNRP」と表記する。例えば、ノード「A」に割り当たるマスタ鍵は、「0-0K00」、「0-0K01」、「0-0K10」となる。全ての子ノードが無効化ノードである場合には、そのノードに割り当たるマスタ鍵は使用されないため、割り当てる必要がない。さらに、全ての子ノードが無効化ノードでない場合には、1つ上のレイヤの鍵を使用することができるため、ルートを除く各ノードには、NRPが「00」に対応するマスタ鍵は必要ない。

【0386】

また、各リーフには、以下のようにして、複数のマスタ鍵を割り当てる。リーフからルートに至るパス上に位置するノードに割り当たっている全てのマスタ鍵のうち、そのリーフが無効化されているときのNRPに対応するマスタ鍵を除いた鍵を割り当てる。例えば、リーフ「D」に割り当たるマスタ鍵は、「0-0K00」、「0-0K01」、「1-0K01」となる。図43(a)にて、各ノードが有するマスタ鍵を示す。

【0387】

なお、各リーフに割り当たる複数のマスタ鍵からなる情報をマスタ鍵セットと呼ぶ。図42では、木構造の左から順に、マスタ鍵セット1、マスタ鍵セット2、マスタ鍵セット3、マスタ鍵セット4とする。また、各マスタ鍵セットにて、所有するマスタ鍵を図43(b)にて示す。

【0388】

ここで、コンテンツ鍵に暗号化に使用するマスタ鍵の選択方法について、説明する。まず、各マスタ鍵セットが無効化されていない場合には、マスタ鍵「0-0K00」を用いて、コンテンツ鍵「CK」を暗号化し、暗号化コンテンツE_nc(0-0K00, CK)を生成する。マスタ鍵「0-0K00」は、全てのマスタ鍵セットにて所有しているため、どのマスタ鍵セットを用いても、暗号化コンテンツE_nc(0-0K00, CK)の復号は可能である。つまり、コンテンツの復号が可能となる。

【0389】

次に、あるマスタ鍵セットが無効化された場合での、マスタ鍵の選択方法について説明する。ここでは、無効化するマスタ鍵セットをマスタ鍵セット2とする。マスタ鍵セット2を無効する場合、無効化ノードは、ノード「A」、「B」、「E」となる。次に、リーフを除く各無効化ノードに対して、そのノードのノード無効化パターンに対応するマスタ鍵を、コンテンツ鍵を暗号化するためのマスタ鍵として選択する。ここでは、ノード「A」から、マスタ鍵「0-0K10」が選択され、さらに、ノード「B」から、マスタ鍵「1-0K

01」が選択される。選択されたマスタ鍵「 $0_0 K_{10}$ 」、「 $1_0 K_{01}$ 」を用いて、暗号化コンテンツ鍵E nc ($0_0 K_{10}$ 、CK) 及びE nc ($1_0 K_{01}$ 、CK) を生成する。無効化されたマスタ鍵セット2は、マスタ鍵「 $0_0 K_{10}$ 」、「 $1_0 K_{01}$ 」を所有していないため、暗号化コンテンツ鍵E nc ($0_0 K_{10}$ 、CK) 又はE nc ($1_0 K_{01}$ 、CK) の復号は不可能である。つまり、コンテンツの復号が不可能となる。他のマスタ鍵セットは、マスタ鍵「 $0_0 K_{10}$ 」、「 $1_0 K_{01}$ 」を所有しているため、暗号化コンテンツ鍵E nc ($0_0 K_{10}$ 、CK) 又はE nc ($1_0 K_{01}$ 、CK) の復号は可能である。つまり、コンテンツの復号が可能となる。

【0390】

なお、説明の便宜上、深さ2の2分木を用いて説明を行ったが、木構造はこれに限定されるものではない。リーフの数が、管理するマスタ鍵セットの数以上となる深さ「m」の「n」分木であればよい。ただし、「m」、「n」は、整数である。

【0391】

以降では、各構成において、プリペイドカードシステム1及びプリペイドカードシステム2と異なる点を中心に説明する。

【0392】

3. 2 記録媒体100Bの構成

ここでは、記録媒体100Bの構成について説明する。

【0393】

記録媒体100Bは、図44に示すROM領域101BとRAM領域102Bとから構成されている。ROM領域101Bは、読み出しのみが可能な領域であり、ライセンスチケット記憶部110Bと配信要求機能記憶部120Bとを有している。RAM領域102Bは、読み出し及び書き込みが可能な領域であり、コンテンツ記憶部130Bと利用状況記憶部140Bとを有している。

【0394】

なお、第1サブシステム11B、・・・、12Bが有する記録媒体は、記録媒体100Bと同様の構成を有しているため、説明は省略する。

【0395】

3. 2. 1 ライセンスチケット記憶部110B

ライセンスチケット記憶部110Bは、図45に一例として示すように、ライセンスチケットテーブルT100Bを有している。

【0396】

ライセンスチケットテーブルT100Bにおけるデータ構造の構成は、第1及び第2の実施の形態で示したライセンスチケットテーブルT100のチケット用暗号化マスタ鍵が、チケット用暗号化マスタ鍵セットに変更される。チケット用暗号化マスタ鍵セットは、マスタ鍵セットをデバイス鍵にて暗号化した情報である。

【0397】

なお、WKS1、WKS2、・・・、WKS10がマスタ鍵セットである。

【0398】

3. 2. 2 配信要求機能記憶部120B

配信要求機能記憶部120Bは、第2の実施の形態で示した配信要求機能記憶部120Aと同様に取得可能コンテンツ一覧画面情報、利用形態選択画面情報、レンタル用チケット選択画面情報、購入用チケット選択画面情報、及び配信要求プログラムを記憶している。

【0399】

ここで、第1の実施の形態で示した配信要求プログラムとは、購入処理における動作がことなる。ここでは、その異なる点について、第1の実施の形態で示した図15を用いて、説明する。

【0400】

図15に示すステップS425を、チケット用暗号化マスタ鍵セットの復号し、マスタ

鍵セットを取得するよう変更する。また、ステップS430を実行する前に、取得したマスタ鍵セットと、コンテンツ取得処理にて受信した配信コンテンツ情報に含まれるインデックス情報とを用いて、復号に使用するマスタ鍵を取得するステップを追加する。

【0401】

このステップの実行後、図15に示すステップS430以降を実行する。

【0402】

3.2.3 コンテンツ記憶部130B

コンテンツ記憶部130Bは、第2の実施の形態で示したコンテンツ記憶部130Aと同様の構成であるが、レンタルコンテンツ記憶部131Bにて、暗号化コンテンツの記憶方法のみが、第2の実施の形態と異なる。図46に示すように、レンタルコンテンツ記憶部131Bは、インデックス情報と暗号化コンテンツ鍵からなる組と、暗号化コンテンツとをコンテンツIDと対応付けて記憶している。ここで、インデックス情報は、暗号化コンテンツ鍵を復号に使用すべきマスタ鍵の情報、つまり、コンテンツ鍵の暗号化に使用したマスタ鍵に情報である。なお、インデックス情報と暗号化コンテンツ鍵との組からなる数は、全てのマスタ鍵セットが有効である場合には、1つであるが、無効化されたマスタ鍵セットが存在する場合には、無効化時に選択されたマスタ鍵の数となる。例えば、図46では、全てのマスタ鍵セットが有効である場合を示しており、インデックス情報「Ind1」は、全マスタ鍵セットが有するマスタ鍵の情報となる。

【0403】

3.2.4 利用状況記憶部140B

利用状況記憶部140Bは、第1の実施の形態で示した利用状況記憶部140と同様に利用状況テーブルT150Bを有している。利用状況テーブルT150Bのデータ構造は、利用状況テーブルT150と同様であるため、説明は省略する。

【0404】

3.3 再生装置200Bの構成

ここでは、再生装置200Bの構成について説明する。

【0405】

再生装置200Bは、図47に示すように、デバイス鍵記憶部201B、時計部202B、配信要求処理部203B、再生処理部204B、入力部205B、出力部206B、第1入出力部207B、第2入出力部208B及びリモコン210Bとから構成されている。

【0406】

再生装置200Bは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置200Bは、その機能を達成する。

【0407】

また、再生装置200Bは、図示していないが、出力部206Bを用いて、テレビと接続されている。なお、再生装置200Bと接続されるものは、テレビに限定はされない。再生装置200Bより出力される映像、音声、又は双方を出力できる装置であればよい。

【0408】

なお、第1サブシステム11B、・・・、12Bが有する再生装置は、再生装置200Bと同様の構成を有しているため、説明は省略する。

【0409】

3.3.1 デバイス鍵記憶部201B

デバイス鍵記憶部201Bは、第2の実施の形態で示したデバイス鍵記憶部201Aと同様であるため、説明は省略する。

【0410】

3.3.2 時計部202B

時計部202Bは、第1の実施の形態で示した時計部202Aと同様であるため、説明は省略する。

【0411】

3.3.3 配信要求処理部203B

配信要求処理部203Bは、リモコン210Bより入力部205Bを介して、コンテンツ配信要求の開始を示す配信要求開始指示情報を受け取る。配信要求処理部203Bは、配信要求開始指示情報を受け取ると、記録媒体100Bより第2入出力部208Bを介して、配信要求機能を読み出し、読み出した配信要求機能を実行する。以下、配信要求処理部203Bが実行する配信要求機能について、第1の実施の形態と異なる点を中心に詳細に説明する。

【0412】

異なる点は、購入時において、配信コンテンツ情報の受信後に行う暗号化コンテンツ鍵及び暗号化コンテンツ鍵の復号における動作が異なる。以下に、配信コンテンツ情報受信後の動作について説明する。

【0413】

配信要求処理部203Bは、コンテンツ提供装置400Bより、配信コンテンツ情報を受信する。ここで、配信コンテンツ情報は、コンテンツIDと、インデックス情報と暗号化コンテンツ鍵との組と、暗号化コンテンツとからなる情報である。ただし、インデックス情報と暗号化コンテンツ鍵との組は、全マスタ鍵セットが有効である場合には、1つであり、無効化されたマスタ鍵が存在する場合には、無効化時に選択されたマスタ鍵の数となる。

【0414】

また、配信コンテンツ情報の受信が完了後、受信完了日時を時計部202Bより取得し、一時的に記憶する。次に、一時的に記憶している購入用ライセンスチケット情報に対応するライセンスチケットに含まれるチケット用暗号化マスタ鍵セットを復号し、マスタ鍵セットを取得する。取得したマスタ鍵セットと、受信した配信コンテンツ情報に含まれるインデックス情報及び暗号化コンテンツ鍵とを用いて、暗号化コンテンツ鍵を復号し、コンテンツ鍵を取得する。取得したコンテンツ鍵を用いて、受信した配信コンテンツ情報に含まれる暗号化コンテンツを復号することにより、コンテンツを取得し、取得したコンテンツを記録媒体100Bの購入コンテンツ記憶部132へ格納する。

【0415】

配信要求処理部203Bは、一時的に記憶している購入用ライセンスチケット情報と、利用形態と、時計部202Bより取得した配信コンテンツ情報の受信完了日時を用いて、利用状況テーブルT150Bの更新を行う。更新方法は、第1の実施の形態で示した方法と同様であるため、説明は省略する。

【0416】

3.3.4 再生処理部204B

再生処理部204Bは、再生装置200Bに記録媒体100Bが装着されている状態で、コンテンツの再生を行う。

【0417】

再生処理部204Bは、第1の実施の形態で示した再生処理部204と同様であるため、説明は省略する。

【0418】

ただし、レンタルコンテンツを再生する場合には、チケット用暗号化マスタ鍵セットを復号し、マスタ鍵セットを取得し、取得したマスタ鍵セットと、インデックス情報とを用いて、暗号化コンテンツ鍵の復号を行い、コンテンツ鍵を取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツの復号を行う。

【0419】

3.3.5 入力部205B

入力部205Bは、第1の実施の形態で示した入力部205と同様であるため、説明は

省略する。

【0420】

3. 3. 6 出力部206B

出力部206Bは、第1の実施の形態で示した出力部206と同様であるため、説明は省略する。

【0421】

3. 3. 7 第1出入力部207B

第1出入力部207Bは、第1の実施の形態で示した第1出入力部207と同様であるため、説明は省略する。

【0422】

3. 3. 8 第2出入力部208B

第2出入力部208Bは、第1の実施の形態で示した第2出入力部208と同様であるため、説明は省略する。

【0423】

3. 3. 9 リモコン210B

リモコン210Bは、第1の実施の形態で示したリモコン210と同様であるため、説明は省略する。

【0424】

3. 4 ライセンスチケット生成装置300Bの構成

ここでは、ライセンスチケット生成装置300Bの構成について説明する。

【0425】

ライセンスチケット生成装置300Bは、図48に示すデバイス鍵記憶部301B、暗号鍵記憶部302B、マスタ鍵生成部303B、チケット用暗号化部304B、ライセンスチケット生成部305B、書込部306B、出力用暗号化部307B、チケット情報記憶部309B、送受信部320B及びライセンスチケット変更部321Bとから構成されている。

【0426】

ライセンスチケット生成装置300Bは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モ뎀などから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ライセンスチケット生成装置300Bは、その機能を達成する。

【0427】

ライセンスチケット生成装置300Bは、木構造の生成及び複数のマスタ鍵の生成を行い、生成した木構造のリーフ以外の各ノードへ生成したマスタ鍵を割り当てる。リーフには、マスタ鍵セットを割り当てる。なお、マスタ鍵及びマスタ鍵セットが割り当てられた木構造を管理用木構造と呼ぶ。

【0428】

さらに、デバイス鍵を用いて、各マスタ鍵セットより暗号化マスタ鍵を生成し、生成した暗号化マスタ鍵セットを用いて、ライセンスチケットを生成する。さらに、生成したライセンスチケットを記録媒体に書き込む。また、生成したライセンスチケットを記録媒体に書き込む動作を繰り返すことにより、ライセンスチケットが書き込まれた記録媒体の大規模生産を行う。

【0429】

また、コンテンツ提供装置400Bより、コンテンツの復号には利用しないマスタ鍵セットを示すマスタ鍵セット無効化情報を受信し、受信したマスタ鍵セット無効化情報を用いて、ライセンスチケットの生成を行う。

【0430】

3. 4. 1 デバイス鍵記憶部301B

デバイス鍵記憶部301Bは、第1の実施の形態にて示したデバイス鍵記憶部301と同様であるため、説明は省略する。

【0431】

3.4.2 暗号鍵記憶部302B

暗号鍵記憶部302Bは、マスタ鍵生成部303Bにて生成された管理用木構造を共通鍵暗号により暗号化するための暗号鍵「K」を記憶している。

【0432】

3.4.3 マスタ鍵生成部303B

マスタ鍵生成部303Bは、木構造の生成及び、乱数を用いて、マスタ鍵の生成を行う。生成したマスタ鍵を生成した木構造のリーフ以外のノードへ割り当て、さらに、リーフには、マスタ鍵セット「WKS1」、「WKS2」、・・・、「WKS10」を割り当て、管理用木構造を生成する。割り当てられたマスタ鍵セットをチケット用暗号化部304Bへ出力し、生成した管理用木構造を出力用暗号化部307Bへ出力する。

【0433】

3.4.4 チケット情報記憶部309B

チケット情報記憶部309Bは、ライセンスチケットテーブルT100B及び利用状況テーブルT150Bを記憶する領域を備えている。

【0434】

チケット情報記憶部309Bにて記憶されているライセンスチケットテーブルT100B及び利用状況テーブルT150Bが記録媒体100Bへ書き込まれることになる。

【0435】

また、利用状況テーブルT150Bを形成するライセンスチケット利用情報は、利用番号と利用状態に「未利用」が記録されており、他の項目は空白である。

【0436】

また、チケット情報記憶部309Bは、配信要求機能を予め記憶している。

【0437】

3.4.5 チケット用暗号化部304B

チケット用暗号化部304Bは、デバイス鍵記憶部301Bにて記憶されているデバイス鍵「DK」を用いて、マスタ鍵生成部303Bより受け取ったマスタ鍵セットを共通鍵暗号で、それぞれ暗号化することにより、チケット用暗号化マスタ鍵セットE_{nc} (DK、WKS1)、E_{nc} (DK、WKS2)、・・・、E_{nc} (DK、WKS10)を生成し、生成した各チケット用暗号化マスタ鍵セットを記憶する。

【0438】

3.4.6 ライセンスチケット生成部305B

ライセンスチケット生成部305Bは、利用可能コンテンツIDとして記録するコンテンツID及び、レンタルと購入との組からなる利用規則を予め記憶している。

【0439】

ライセンスチケット生成部305Bは、チケット用暗号化部304Bにて記憶されているチケット用暗号化マスタ鍵セットと、予め記憶している利用可能コンテンツIDとして記録するコンテンツID及び利用規則とを用いて、ライセンスチケットテーブルT100Bを生成し、生成したライセンスチケットテーブルT100Bをチケット情報記憶部309Bへ格納する。

【0440】

さらに、利用状況テーブルT150Bをも生成し、生成した利用状況テーブルT150Bをチケット情報記憶部309Bへ格納する。

【0441】

3.4.7 ライセンスチケット変更部321B

ライセンスチケット変更部321Bは、コンテンツ提供装置400Bより送受信部320Bを介して、マスタ鍵セット無効化情報を受信すると、チケット情報記憶部309Bにて記憶しているライセンスチケットテーブルT100Bより、受信したマスタ鍵セット無

効化情報を用いて、利用できない暗号化マスタ鍵セットを含むライセンスチケットを削除して、ライセンスチケットテーブルT100Bを更新する。さらに、チケット情報記憶部309Bにて記憶している利用状況テーブルT150Bより、削除されたライセンスチケットに対応するライセンスチケット利用情報を削除して、利用状況テーブルT150Bを更新する。

【0442】

3. 4. 8 書込部306B

書込部306Bは、チケット情報記憶部309Bにて記憶しているライセンスチケットテーブルT100Bと、利用状況テーブルT150Bと、配信要求機能とを記録媒体100Bへ書き込む。

【0443】

ここで、ライセンスチケットテーブルT100B、利用状況テーブルT150B、配信要求機能をプレス加工にて、記録媒体100Bへの書き込むことにより、低コストにて生産が可能となる。

【0444】

3. 4. 9 出力用暗号化部307B

出力用暗号化部307Bは、暗号鍵記憶部302Bにて記憶されてる暗号鍵「K」を用いて、マスタ鍵生成部303Bより受け取った管理用木構造を共通鍵暗号で、それぞれ暗号化し、暗号化された管理用木構造を送受信部320Bを介してコンテンツ提供装置400Bへ送信する。

【0445】

3. 4. 10 送受信部320B

送受信部320Bは、出力用暗号化部307Bより受け取った情報をコンテンツ提供装置400Bへ送信する。また、コンテンツ提供装置400Bより受信した情報をライセンスチケット生成部305Bへ出力する。

【0446】

3. 5 コンテンツ提供装置400Bの構成

ここでは、コンテンツ提供装置400Bの構成について説明する。

【0447】

コンテンツ提供装置400Bは、図49に示す復号鍵記憶部401B、マスタ鍵記憶部402B、コンテンツ関連情報記憶部403B、配信データ記憶部404B、復号部406B、入力部407B、コンテンツ鍵生成部408B、暗号化部409B、コンテンツ読込部410B、配信処理部411B、第1送受信部420B、第2送受信部421B及び無効化処理部422Bとから構成されている。

【0448】

コンテンツ提供装置400Bは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、モデムなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、コンテンツ提供装置400Bは、その機能を達成する。

【0449】

なお、コンテンツ提供装置400Bは、コンテンツIDと、コンテンツとからなるコンテンツ媒体の着脱が可能であり、コンテンツの暗号化を行う場合には、コンテンツ媒体が装着された状態で行う。

【0450】

3. 5. 1 復号鍵記憶部401B

復号鍵記憶部401Bは、第1の実施の形態にて示した復号鍵記憶部401と同様であるため、説明は省略する。

【0451】

3. 5. 2 マスタ鍵記憶部402B

マスタ鍵記憶部402Bは、復号部406Bにて復号された管理用木構造を記憶する領域を備えている。また、利用中であるマスタ鍵のインデックス情報を記憶する領域をも備えている。

【0452】

3. 5. 3 コンテンツ関連情報記憶部403B

コンテンツ関連情報記憶部403Bは、第1の実施の形態で示したコンテンツ関連情報記憶部403と同様に、コンテンツ関連情報テーブルT400Bを有している。

【0453】

コンテンツ関連情報テーブルT400Bは、コンテンツ関連情報テーブルT400と同様であるため、説明は省略する。

【0454】

3. 5. 4 配信データ記憶部404B

配信データ記憶部404Bは、第1の実施の形態にて示した配信データ記憶部404と同様に、暗号化コンテンツ管理テーブルT410Bを有している。

【0455】

暗号化コンテンツ管理テーブルT410Bは、暗号化コンテンツ管理テーブルT410と同様であるため、説明は省略する。

【0456】

なお、暗号化コンテンツ情報に含まれる暗号化コンテンツ鍵には、インデックス情報とそれに対応する暗号化コンテンツ鍵との組が記憶されている。インデックス情報とそれに対応する暗号化コンテンツ鍵との組は、全マスタ鍵セットが有効である場合には1つであり、無効化されたマスタ鍵セットが存在する場合には、無効化時に選択されたマスタ鍵の個数となる。

【0457】

3. 5. 5 第1送受信部420B

第1送受信部420Bは、ライセンスチケット生成装置300Bより、暗号化された管理用木構造を受信し、受信した暗号化された管理用木構造を復号部406Bへ出力する。

【0458】

また、無効化処理部422Bよりマスタ鍵セット無効化情報を受け取ると、受け取ったマスタ鍵セット無効化情報をライセンスチケット生成装置300Bへ送信する。

【0459】

3. 5. 6 復号部406B

復号部406Bは、受信部405Bより暗号化された管理用木構造を受け取ると、復号鍵記憶部401Bより復号鍵を取得し、取得した復号鍵を用いて、暗号化された管理用木構造の復号を行い、復号された管理用木構造をマスタ鍵記憶部402Bへ書き込む。さらに、初期状態として、全マスタ鍵が有効である場合に使用するマスタ鍵のインデックス情報をもマスタ鍵記憶部402Bへ書き込む。

【0460】

3. 5. 7 入力部407B

入力部407Bは、暗号化開始情報を受け付け、受け付けた暗号化開始情報をコンテンツ鍵生成部408Bへ出力する。

【0461】

また、マスタ鍵セット無効化情報を受け付け、受け付けたマスタ鍵セット無効化情報を無効化処理部422Bへ出力する。

【0462】

3. 5. 8 コンテンツ鍵生成部408B

コンテンツ鍵生成部408Bは、第1の実施の形態で示したコンテンツ鍵生成部408と同様であるため、説明は省略する。

【0463】

3. 5. 9 無効化処理部422B

無効化処理部422Bは、入力部407Bより、マスタ鍵セット無効化情報を受け取ると、受け取ったマスタ鍵セット無効化情報を用いて、管理用木構造に対して、利用できないマスタ鍵セット及び利用できないマスタ鍵セットからルートまでに至るノードの無効化を行い、さらには、利用できるマスタ鍵の選択を行う。

【0464】

また、暗号化コンテンツ管理テーブルT410Bの暗号化コンテンツ鍵を、対応するインデックス情報と、管理機構構造とを用いて、コンテンツ鍵を取得し、取得したコンテンツ鍵を、選択されたマスタ鍵を用いて、暗号化し、暗号化コンテンツ鍵を生成する。なお、暗号化コンテンツ鍵の生成は、選択されたマスタ鍵分を行う。生成された暗号化コンテンツ鍵にて、情報を更新する。この動作を暗号化コンテンツ管理テーブルT410Bに記録されている全ての情報に対して行う。また、選択されたマスタ鍵のインデックス情報をマスタ鍵記憶部402Bへ書き込む。

【0465】

さらに、受け取ったマスタ鍵セット無効化情報を第1送受信部420Bを介してライセンスチケット生成装置300Bへ送信する。

【0466】

3. 5. 10 暗号化部409B

暗号化部409Bは、コンテンツ鍵生成部408Bよりコンテンツ鍵を受け取ると、コンテンツ取得開始情報をコンテンツ読込部410Bへ出力し、コンテンツ読込部410BよりコンテンツIDとコンテンツのデータを受け取る。

【0467】

さらに、受け取ったコンテンツ鍵を用いて、コンテンツのデータを共通鍵暗号で暗号化することにより、暗号化コンテンツを生成する。

【0468】

暗号化部409Bは、マスタ鍵記憶部402Bよりインデックス情報と、インデックス情報と対応するマスタ鍵を取得し、取得したマスタ鍵を用いて、コンテンツ鍵を共通鍵暗号で、暗号化することにより、暗号化コンテンツ鍵を生成する。

【0469】

また、暗号化部409Bは、コンテンツ関連情報テーブルT400Bより、コンテンツ読込部410Bより受け取ったコンテンツIDに対応するコンテンツ名及び定価を取得する。

【0470】

暗号化部409Bは、生成した暗号化コンテンツと、取得したインデックス情報と生成した暗号化コンテンツ鍵との組と、コンテンツ読込部410Bより受け取ったコンテンツIDと、コンテンツ関連情報テーブルT400Bより取得したコンテンツ名及び定価とかなる組を配信データ記憶部404Bへ書き込む。

【0471】

3. 5. 11 コンテンツ読込部410B

コンテンツ読込部410Bは、第1の実施の形態にて示したコンテンツ読込部410と同様であるため、説明は省略する。

【0472】

3. 5. 12 配信処理部411B

配信処理部411Bは、第2送受信部421Bを介して再生装置200Bよりコンテンツ一覧要求情報を受信すると、暗号化コンテンツ管理テーブルT410Bを用いて、コンテンツ一覧情報を生成し、再生装置200Bへ第2送受信部421Bを介して送信する。

【0473】

配信処理部411Bは、第2送受信部421Bを介して再生装置200Bよりコンテンツ配信要求情報を受信すると、暗号化コンテンツ管理テーブルT410Bより、受信したコンテンツ配信要求情報に含まれるコンテンツIDと一致するコンテンツID、1以上の

インデックス情報と暗号化コンテンツ鍵との組、及び暗号化コンテンツを取得し、取得したコンテンツID、1以上のインデックス情報と暗号化コンテンツ鍵との組、及び暗号化コンテンツを用いて、配信コンテンツ情報を生成し、生成した配信コンテンツ情報を再生装置200Bへ第2送受信部421Bを介して送信する。

【0474】

3. 5. 1.3 第2送受信部421B

第2送受信部421Bは、第1の実施の形態にて示した送受信部412と同様である為、説明は省略する。

【0475】

3. 6 プリペイドカードシステム3の動作

ここでは、プリペイドカードシステム3の動作について説明する。

【0476】

3. 6. 1 ライセンスチケット生成時の動作概要

ライセンスチケット生成時の動作概要は、第1の実施の形態において示した図25の流れ図と同様であるため、説明は省略する。

【0477】

ただし、ライセンスチケット生成装置300Bがコンテンツ提供装置400Bへ送信する情報は、暗号化された管理木構造である。また、コンテンツ提供装置400Bは、受信した暗号化された管理木構造を復号する。

【0478】

3. 6. 2 コンテンツ配信要求時の動作概要

コンテンツ配信要求時の動作概要は、第1の実施の形態において示した図26の流れ図と同様であるため、説明は省略する。

【0479】

3. 6. 3 ライセンスチケット生成処理の動作

ここでは、ライセンスチケット生成装置300Bにて行われるライセンスチケット生成処理について、図50に示す流れ図を用いて説明する。

【0480】

ライセンスチケット生成装置300Bは、木構造及びマスタ鍵の生成、生成したマスタ鍵をリーフ以外のノードへの割当、及びマスタ鍵セットの生成を行い、管理木構造を生成する（ステップS3000）。生成した管理木構造を暗号化し（ステップS3010）、暗号化した管理木構造をコンテンツ提供装置400Bへ送信する（ステップS3020）。次に、生成したマスタ鍵セットを暗号化し、チケット用暗号化マスタ鍵セットを生成する（ステップS3030）。生成したチケット用暗号化マスタ鍵セットと、記憶しているコンテンツID及び利用規則とを用いて、ライセンスチケットテーブルT100Bを生成し、生成したライセンスチケットテーブルT100Bをチケット情報記憶部309Bへ格納する（ステップS3040）。さらに、ライセンス利用状況情報からなる利用状況テーブルT150Bを生成し、生成した利用状況テーブルT150Bをチケット情報記憶部309Bへ格納する（ステップS3050）。

【0481】

チケット情報記憶部309Bにて記憶しているライセンスチケットテーブルT100B及び利用状況テーブルT150Bと、予め記憶している配信要求機能とを記録媒体100Bへ書き込む（ステップS3060）。

【0482】

なお、ステップS3060のみを繰り返すことで、記録媒体を複数生成することができる。

【0483】

3. 6. 4 ライセンスチケット変更処理の動作

ライセンスチケット生成装置300Bが行うライセンスチケット変更処理の動作は、図39の流れ図と同様であるため説明は省略する。

【0484】

ただし、ライセンスチケット生成装置300Aが、コンテンツ提供装置400Aより受信する情報は、マスタ鍵セット無効化情報であり、ライセンスチケット生成装置300Aは、受信したマスタ鍵セット無効化情報を用いて、ライセンスチケットテーブルT100Bの更新を行い、さらには、利用状況テーブルT150Bの更新を行うこととなる。

【0485】

これにより、チケット情報記憶部309Bの内容が更新される。なお、ライセンスチケット生成処理における書き込みステップのみを行うことで、更新された内容を記憶媒体に書き込むことが可能となる。

【0486】

3. 6. 5 コンテンツ取得処理の動作

再生装置200Bにおいて、コンテンツ取得時に行われるコンテンツ取得処理は、第1の実施の形態にて示した図28の流れ図と同様であるため、説明は省略する。

【0487】

3. 6. 6 再生処理の動作

再生装置200Bにて行われる再生処理は、第1の実施の形態にて示した図29の流れ図からの変更点のみ説明する。

【0488】

図29に示すステップS860を、取得したライセンスチケット利用情報含まれる利用番号に対応するライセンスチケットに含まれるチケット用マスタ鍵セットを取得するよう変更する。また、ステップS870を取得したチケット用マスタ鍵セットを復号し、マスタ鍵セットを取得するよう変更する。また、ステップS880を、暗号化コンテンツ鍵とインデックス情報との組と、暗号化コンテンツを取得するよう変更し、ステップS890を、取得したインデックス情報と、ステップS870にて取得したマスタ鍵セットとを用いて、暗号化コンテンツ鍵を復号し、コンテンツ鍵を取得するよう変更する。

【0489】

3. 6. 7 利用状態確認処理の動作

再生処理時に行われる利用状態確認処理は、第1の実施の形態にて示した図30の流れ図と同様であるため、説明は省略する。

【0490】

3. 6. 8 暗号化コンテンツ生成処理の動作

コンテンツ提供装置400にて行われるコンテンツの暗号化の動作は、第1の実施の形態にて示した図31の流れ図と同様であるため、説明は省略する。

【0491】

ただし、ステップS1150では、マスタ鍵記憶部402Bにて記憶しているインデックス情報に基いて、マスタ鍵を取得することとなる。また、取得したマスタ鍵が複数ある場合には、ステップS1160では、複数の暗号化コンテンツ鍵が生成されることとなる。

【0492】

3. 6. 9 マスタ鍵無効化処理

コンテンツ提供装置400Bにて行われるマスタ鍵無効化処理は、第2の実施の形態にて示した図40の流れ図からの変更点のみ説明する。

【0493】

ステップS2100では、マスタ鍵セット無効化情報を受け付ける。次に、ステップS2110では、受け付けたマスタ鍵セット無効化情報を用いて、管理用木構造に対して、利用できないマスタ鍵セット及び利用できないマスタ鍵セットからルートまでに至るノードの無効化を行い、さらには、利用できるマスタ鍵の選択を行う。

【0494】

また、ステップS2120では、選択されたマスタ鍵を用いて、コンテンツ鍵を暗号化し、暗号化コンテンツ鍵を生成し、生成した暗号化コンテンツ鍵にて、暗号化コンテンツ

管理テーブルT410Bの更新を行う。

【0495】

さらに、ステップS2130を行う前に、選択されたマスタ鍵のインデックス情報をマスタ鍵記憶部402Bへ書き込むステップを追加する。

【0496】

3. 7 第3の実施の形態のまとめ

以上、説明したようにプリペイドカードシステム3においては、記録媒体100Bにてマスタ鍵が暗号化された暗号化マスタ鍵を記憶しており、コンテンツ提供装置400Bにてコンテンツ毎に、暗号化コンテンツ鍵及び暗号化コンテンツを暗号化コンテンツ管理テーブルを用いて記憶している。コンテンツ毎に生成された暗号化コンテンツ鍵は、記録媒体100Bに記憶している暗号化マスタ鍵を復号して、取得したマスタ鍵を用いて復号することが可能である。これは、利用者がコンテンツ提供装置400Bに対して配信要求できるコンテンツを限定しないことを意味している。つまり、利用者は、記録媒体100Bの購入時に購入するコンテンツを決定しておく必要がなく、記録媒体100Bの購入後、自由にコンテンツを選ぶことが可能となる。

【0497】

また、記録媒体100Bに、利用規則として期間を記憶しておくことにより、利用者は、記憶されている期間を指定して、コンテンツを入手した場合には、指定した期間内において、入手したコンテンツを視聴することができる。

【0498】

また、記録媒体100Bに入手可能なコンテンツIDとして、ワイルドカード表記を含めたコンテンツIDを記憶しておくことにより、利用者は、記憶されているワイルドカード表記を含めたコンテンツIDを用いて、コンテンツ提供装置400Bにて有している多数のコンテンツより、入手可能なコンテンツを抽出し、抽出した結果より、コンテンツを自由に選ぶことができる。

【0499】

また、記録媒体100Bの購入時に、コンテンツのレンタル又は購入に関する料金を支払っているため、インターネットを用いた決済方法を実現するためのPKIや、料金を管理するセンタを必要としない。そのため、煩雑な処理を行う必要がないため、簡単な仕組みでシステムを構成することができる。また、他の決済方法として、キオスク端末にて、購入コンテンツを記録媒体にて記録し販売する決済方法があるが、この場合には、購入コンテンツは予め決めておく必要がある。しかしながら、上記に記述したように、記録媒体の購入時には、購入するコンテンツを決めておく必要がないため、キオスク端末において利用される決済方法を用いる必要がない。

【0500】

また、コンテンツ鍵を暗号化するために用いるマスタ鍵を、コンテンツの再生が可能な再生装置が持つデバイス鍵を用いて、共通鍵暗号で暗号化を行うことにより、コンテンツの再生が不可能な装置にて、マスタ鍵を読みとて暴露するのを防止することができる。

【0501】

また、暗号化コンテンツ鍵の暗号化方法にBEを用いていることにより、万一、マスタ鍵が暴露された場合には、その暴露されたマスタ鍵を無効化することにより、コンテンツを復号できないようにすることができ、セキュリティが向上される。また、マスタ鍵を木構造にて管理することにより、配信される暗号化コンテンツ鍵は、必要最低限の個数のみでよいため、配信する情報量が軽減される。

【0502】

4. まとめ

以上説明したように、本発明によれば、プリペイドカードシステムは、コンテンツ提供装置より暗号化コンテンツが配信されている場合でも、暗号化マスタ鍵が記憶された記録媒体を利用することにより、コンテンツを自由に選ぶことが可能となる。

【0503】

また、記録媒体に、利用規則として期間を記憶しておくことにより、利用者は、記憶されている期間を指定して、コンテンツを入手した場合には、指定した期間内において、入手したコンテンツを視聴することができる。

【0504】

また、記録媒体に入手可能なコンテンツIDとして、ワイルドカード表記を含めたコンテンツIDを記憶しておくことにより、利用者は、記憶されているワイルドカード表記を含めたコンテンツIDを用いて、コンテンツ提供装置にて有している多数のコンテンツより、入手可能なコンテンツを抽出し、抽出した結果より、コンテンツを自由に選ぶことができる。

【0505】

また、記録媒体の購入時に、コンテンツのレンタル又は購入に関する料金を支払っているため、インターネットを用いた決済方法を実現するためのPKIや、料金を管理するセンタを必要としない。そのため、煩雑な処理を行う必要がないため、簡単な仕組みでシステムを構成することができる。

【0506】

また、コンテンツ鍵を暗号化するために用いるマスタ鍵を、コンテンツの再生が可能な再生装置が持つデバイス鍵を用いて、共通鍵暗号で暗号化を行うことにより、コンテンツの再生が不可能な装置にて、マスタ鍵を読みとて暴露するのを防止することができる。

【0507】

また、暗号化コンテンツ鍵の暗号化方法にBEを用いていることにより、万一、マスタ鍵が暴露された場合には、その暴露されたマスタ鍵を無効化することにより、コンテンツを復号できないようにすることができ、セキュリティが向上される。さらには、マスタ鍵を木構造にて管理することにより、配信する暗号化コンテンツ鍵を必要最低限の個数とすることことができ、配信する情報量が軽減される。

【0508】

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下の場合も本発明に含まれる。

【0509】

(変形例)

(1) 上記の実施の形態では、ライセンスチケットの利用規則をレンタル時の日数と購入時の利用金額との2つの項目に分けたが、これに限定されない。利用規則を金額のみとしてもよい。

【0510】

このとき、1日のレンタル料金を予め設定しておき、レンタル用チケット選択画面を表示する際に、ライセンスチケットに示されている金額をもとに、各ライセンスチケットでレンタル可能な期間を算出し、算出結果を用いればよい。

【0511】

(2) ライセンスチケットを利用金額の残額を用いて管理してもよい。この場合の実現方法を以下に説明する。

【0512】

残額を管理する残額管理領域を記録媒体のRAM領域に備え、さらに、利用状況テーブルには、レンタル期間項目を追加する。

【0513】

再生装置は、コンテンツのレンタル又は購入を行う際に、残額管理領域に記憶されている残額を表示する。レンタル時には、レンタル期間を受け付け、受け付けた期間よりレンタル料金を算出し、算出したレンタル料金が残額内であるか否かを判断する。残額内である場合には、コンテンツの配信要求を行い、配信コンテンツ情報を受信し、受信完了後、利用状況テーブルを更新する。利用状況テーブルの更新の際、新たに設けたレンタル期間項目に受け付けたレンタル期間を記録する。また、利用後の残額を算出し、算出された新たな残額を用いて、残額管理領域の内容を更新する。

【0514】

購入時には、購入を希望するコンテンツの定価と残額を比較し、定価が残額内である場合には、コンテンツの配信要求を行い、配信コンテンツ情報を受信し、受信完了後、利用状況テーブルを更新する。利用状況テーブルの更新の際、新たに設けたレンタル期間項目は、空白とする。

【0515】

(3) 上記(2)において、残額管理をコンテンツ提供者側で行ってもよい。

【0516】

このとき、記録媒体には、管理IDを付加され、映画会社では、残額を管理する残額管理装置を備え、残額を管理IDと対応付けて管理している。

【0517】

再生装置では、コンテンツ配信要求情報を送信する際に、管理IDと、レンタル及びレンタル日数、又は購入を示す情報を付加して、コンテンツ提供装置へ送信する。コンテンツ提供装置では、受け取った情報を用いて、利用金額を算出する。さらに、受信した管理IDと対応する残額を残額管理装置より取得し、算出された利用金額が、取得した残額内であるか否かを判断し、残額内である場合には、配信コンテンツ情報を送信し、新たな残額を算出し、算出した新たな残額を残額管理装置へ出力し、受信した管理IDに対応する残額の更新をする。また、利用金額が残額を超えている場合には、配信コンテンツ情報の送信及び残額の更新は行わない。

【0518】

なお、残額管理装置にて行う残額管理を、コンテンツ提供装置にて行ってもよいし、ライセンスチケット生成装置にて行ってもよい。

【0519】

(4) 上記(3)において、PDAや携帯電話機などの通信端末を用いて、残額管理装置とネットワーク接続を行い、ネットワーク接続後、通信端末より残額管理装置へ管理IDを送信することにより、残額管理装置より、残額に係る情報を受信し、利用者へ残額の通知を行うようにしてもよい。

【0520】

または、記録媒体に無線タグを備え、この無線タグと通信端末とを用いて、管理IDを残額管理装置へ送信して、残額に係る情報を受信してもよい。

【0521】

(5) 上記(2)において、残額に係る情報を記録媒体の未使用領域である内・外延部に、書き込み・非書き込みを制御して、可視的に残額を記録してもよい。

【0522】

(6) 上記の実施の形態では、再生装置は、再生開始指示情報の受け付け時に、利用状況テーブルの更新を行ったが、これに限定されない。記録媒体を常時、再生装置に装着しておき、定期的に利用状況テーブルの更新をおこなってもよい。

【0523】

または、利用状況テーブルを再生装置内に設けて、定期的に利用状況テーブルの更新を行ってもよい。

【0524】

(7) 利用状況テーブルを暗号化して、記憶してもよい。

【0525】

このとき、デバイス鍵を用いて、共通鍵暗号により利用状況テーブルの暗号化を行う。また、利用状況テーブルの利用時には、デバイス鍵を用いて、復号する。

【0526】

(8) 上記の実施の形態では、暗号化マスタ鍵を生成する際に、デバイス鍵を用いたが、これに限定されない。記録媒体固有の情報を用いて、暗号化マスタ鍵を生成してもよい。または、記録媒体固有の情報とデバイス鍵の両者を用いて、暗号化マスタ鍵を生成してもよい。

【0527】

例えば、記録媒体に固有のID、BCA (Burst Cutting Area) 領域に記録されている情報、Disc毎又はロット毎に異なるDisc鍵、Disc毎に異なるWobble (記録時のアドレス導出用に記録された波形) から得られるデータである。

【0528】

(9) 上記の実施の形態では、ライセンスチケットを記録媒体のROM領域に設けたが、これに限定されない。ライセンスチケットをRAM領域に設けてもよい。

【0529】

(10) ライセンスチケットを、コンテンツ提供者が有する秘密鍵を用いてデジタル署名を施してもよい。これにより、ライセンスチケットの不正な書換を防止することができ、セキュリティが向上する。このとき、記録媒体に映画会社の公開鍵証明書を記録し、再生装置がデジタル署名を検証することとなる。

【0530】

(11) 上記の実施の形態では、ライセンスチケットの未利用・利用済の判断を利用状況テーブルを用いて行ったが、これに限定されない。ROM領域のライセンスチケットに、再生装置より、強力なレーザを照射して、利用しライセンスチケットを消去するようにしてもよい。

【0531】

(12) 上記の実施の形態では、RAM領域の利用状況記憶部には、読み書きの制限を行っていないが、コンテンツの再生が許可されている再生機器（以下、正規機器）しか書き込めないように、デバイス鍵や、コンテンツ提供者と正規機器とが秘密に保持する情報を用いて、暗号化やMAC（メッセージ認証子）を附加してもよい。

【0532】

(13) 上記の実施の形態では、コンテンツ提供者を映画会社としたが、これに限定されない。コンテンツ提供者は、コンテンツを配信する業者若しくは個人であればよい。

【0533】

例えば、レンタルショップ、デジタル放送局、音楽業者である。

【0534】

(14) 上記の実施の形態では、ライセンスチケットを有する記録媒体（以下、プリペイドカード）は、映画会社固有のものであったが、これに限定されない。利用可能コンテンツIDを、コンテンツ提供者を識別する識別子と作品識別子とからなるものとして、コンテンツ提供者を識別する識別子に示されたコンテンツ提供者に固有のプリペイドカードとしてもよい。

【0535】

各ライセンスチケットの利用可能コンテンツIDをレンタルショップを識別するレンタルショップ識別子と、ワイルド表記が可能な作品識別子とからなるものとしてもよい。これにより、レンタルショップ固有のプリペイドカードとすることができる、レンタルショップより、コンテンツのレンタル又は購入が可能となる。

【0536】

また、利用可能コンテンツIDを映画会社識別子又はレンタルショップ識別子と、ワイルド表記を不可とする作品識別子とからなるようにしてもよい。いくつかの決められたコンテンツのみを対象としたプリペイドカードとすることができる、映画会社又はレンタルショップより、これらの決められたコンテンツより選択したコンテンツのレンタル又は購入が可能となる。

【0537】

さらに、利用可能コンテンツIDを映画会社識別子又はレンタルショップ識別子と、ワイルド表記を不可とする作品識別子からなるものとすることにより、著名人によりセレクションされたコンテンツのレンタル又は購入が可能となるプリペイドカードを生成することにより、プリペイドカードに付加価値をつけることも可能となる。

【0538】

または、利用可能コンテンツIDの先頭3桁に対しても、ワイルドカード表記を可能としてもよい。これにより、映画会社、レンタルショップなどコンテンツ提供者を意識することなく、コンテンツのレンタル又は購入が可能となる。

【0539】

(15) 上記の実施の形態では、ライセンスチケットの利用規則をレンタル時の日数と購入時の利用可能金額から構成したが、これに限定されない。

【0540】

利用規則には、ライセンスチケット利用開始から利用できる時間を示す規定時間を記録してもよい。これにより、規定時間内であれば、そのライセンスチケットで利用可能なコンテンツならどれでも視聴が可能となる。例えば、コンテンツ「 BBB 」を視聴後、規定時間内であれば、さらに、別のコンテンツ「 CCC 」の視聴ができる。

【0541】

(16) 再生装置よりコンテンツ提供装置へコンテンツ配信要求情報を送信する際に、個人情報も送信するようにしてもよい。

【0542】

このとき、個人情報は、記録媒体購入時に、販売店にて記録される。再生装置は、ライセンスチケット利用時に、記録された個人情報をコンテンツ提供装置へ送信する。これにより、コンテンツ提供者は、受信した個人情報をマーケティングに利用することができる。

【0543】

ここで、個人情報は、例えば、年齢、性別である。

【0544】

(17) ライセンスチケットに、そのライセンスチケットを用いて、レンタル又は購入したコンテンツの視聴を開始することが可能となる日時を示す視聴開始可能日時を設けてもよい。これにより、封切り前のコンテンツを予め入手することが可能となる。

【0545】

このとき、コンテンツのレンタル又は購入時に、再生装置にて行われる利用状況テーブルの利用開始日時の記録は、以下のようにして行う。時計部より、受信完了日時を取得する。取得した受信完了日時と、利用したライセンスチケットテーブルの視聴開始可能日時とを比較し、視聴開始可能日時が、受信完了日時より過去の日時となっている場合には、受信完了日時を利用開始日時として記録する。また、視聴開始可能日時が、受信完了日時より未来の日時となっている場合には、視聴開始可能日時を利用開始日時として記録する。

【0546】

再生装置は、再生時には、現在の日時と、利用状況テーブルの利用開始日時とを比べて、利用開始日時が未来の日時となっている場合には、それに対応するコンテンツは、再生可能コンテンツ一覧には表示しないように制御する。これにより、利用開始日時となるまで、封切り前のコンテンツの視聴はできない。

【0547】

(18) 暗号化コンテンツ管理テーブルに視聴開始可能日時を設けてもよい。

【0548】

このとき、配信コンテンツ情報に、視聴開始可能日時を付加する。再生装置では、上記(17)と同様の方法にて、利用状況テーブルの利用開始日時の記録を行う。また、再生装置は、再生時も上記(17)と同様の方法にて行う。

【0549】

これにより、コンテンツ提供者は、封切り前のコンテンツを予め配信することが可能となる。また、利用者は、利用開始日時となるまで、封切り前のコンテンツの視聴はできない。

【0550】

(19) コンテンツ提供装置にて、コンテンツ毎の配信要求の状況を管理してもよい。

【0551】

これにより、コンテンツ毎の配信要求の状況を管理することにより、コンテンツのプレス枚数を予測することが可能となり、余剰在庫のリスクが減少する。

【0552】

さらには、T V パッケージ等権利関係が複雑な場合には、余剰在庫のリスク減少は、不要なライセンス料金の支払の減少に繋がる。

【0553】

(20) 上記の実施の形態では、記録媒体は、光ディスクとしたが、これに限定されない。可搬型のメモリカードであってもよい。さらには、I C 機能付メモリカードでもよい。

【0554】

(21) 上記の実施の形態では、配信要求プログラムを再生装置にて実行したが、これに限定されない。記録媒体をI C 機能付メモリカードとし、配信要求プログラムをI C 機能付メモリカードにて実行してもよい。

【0555】

(22) 上記の実施の形態では、配信要求機能記憶部を記録媒体に備えたが、これに限定されない。再生装置に、配信要求機能記憶部を備えてもよい。

【0556】

(23) 再生装置に、配信コンテンツ情報を自動的に受信する機能を設けてもよい。これにより、デジタル放送局などにおいて自動配信される配信コンテンツ情報を受信することが可能となる。

【0557】

記録媒体が装着された再生装置は、デジタル放送局とネットワーク接続し、デジタル放送局より自動配信された配信コンテンツ情報を受信する。受信した配信コンテンツ情報に含まれるコンテンツ I D が、記録媒体に記録されている未利用のライセンスチケットの利用可能コンテンツ I D の条件を満たしている場合に、受信した配信コンテンツ情報を保存する。条件を満たしていない場合には、受信した配信コンテンツ情報を破棄する。

【0558】

利用者は、保存されている配信コンテンツ情報を用いて、視聴したいコンテンツをライセンスチケットを利用して、視聴することが可能となる。

【0559】

(24) 上記の実施の形態では、ライセンス生成装置とコンテンツ提供装置とを専用線にてネットワーク接続したが、これに限定されない。他のネットワーク接続でもよい。例えば、インターネットによるネットワーク接続である。

【0560】

また、再生装置とコンテンツ提供装置とをインターネットによるネットワーク接続としたが、他のネットワーク接続でもよい。例えば、専用線によるネットワーク接続である。

【0561】

(25) 第2の実施の形態において、ライセンスチケット毎に、異なるマスタ鍵を用いたが、これに限定されない。ディスク毎やロット毎に、異なるマスタ鍵を用いてもよい。

【0562】

(26) 近い将来、消費者へネットワーク接続のできる次世代D V D 記録再生装置（以下、「B D レコーダ」という。）の普及が予想される。再生装置は、このB D レコーダであってもよい。

【0563】

(27) 第1及び第2の実施の形態において、ライセンスチケットに記録するマスタ鍵を暗号化して記録したが、これに限定されない。暗号化しないで、マスタ鍵を記録してもよい。

【0564】

また、第3の実施の形態において、ライセンスチケットに記録するマスタ鍵セットを暗号化して記録したが、これに限定されない。暗号化しないで、マスタ鍵セットを記録してもよい。

【0565】

(28) 第1及び第2の実施の形態において、ライセンスチケット生成装置にて生成されたマスタ鍵を暗号化して、コンテンツ提供装置へ送信したが、これに限定されない。暗号化しないで、送信してもよい。または、ライセンスチケット生成装置は、生成したマスタ鍵若しくは暗号化マスタ鍵を記録媒体に格納し、コンテンツ提供装置は、当該記録媒体を用いて、マスタ鍵若しくは暗号化マスタ鍵を受け付けてもよい。

【0566】

または、第3の実施の形態において、ライセンスチケット生成装置にて生成された管理木構造を暗号化して、コンテンツ提供装置へ送信したが、これに限定されない。暗号化しないで、送信してもよい。または、ライセンスチケット生成装置は、生成した管理木構造若しくは暗号化した管理木構造を記録媒体に格納し、コンテンツ提供装置は、当該記録媒体を用いて、管理木構造若しくは暗号化した管理木構造を受け付けてもよい。

【0567】

(29) 上記の実施の形態において、再生時に、利用状況テーブルの更新後、再生可能なコンテンツの情報を抽出したが、これに限定されない。記録媒体に記録されているコンテンツの情報を全て表示し、再生したいコンテンツの情報を受け付け、受け付けたコンテンツの情報に対応するコンテンツが再生可能であるか否かの判断、つまり再生したいコンテンツが、レンタルであるか購入であるかの判断を行い、レンタルである場合には、さらにレンタル期間内であるか否かの判断を行う。再生したいコンテンツが、購入又は、レンタル且つレンタル期間内である場合には再生に係る処理を行い、再生したいコンテンツが、レンタル且つレンタル期間の超過である場合には、再生を行わない。

【0568】

(30) 上記の実施の形態では、コンテンツを購入した場合、暗号化コンテンツを復号し、復号されたコンテンツを記録媒体に格納したが、これに限定されない。コンテンツをレンタルした場合と同様の格納方法で、記録媒体に格納してもよい。

【0569】

このとき、再生装置は、購入したコンテンツの再生を行う度に以下の動作を行う。購入時に使用したライセンスチケットに含まれるチケット用暗号化マスタ鍵を復号し、復号されたマスタ鍵を用いて、暗号化コンテンツ鍵を復号し、復号されたコンテンツ鍵を用いて、暗号化コンテンツを復号し、復号されたコンテンツの再生を行い、再生終了後には、復号されたコンテンツを破棄する。

【0570】

(31) 上記の実施の形態では、コンテンツ記憶部を記録媒体に備えたが、これに限定されない。再生装置にコンテンツ記憶部を備えてもよい。

【0571】

または、コンテンツを利用する度に、再生装置は、コンテンツ提供装置からネットワークを介して、利用するコンテンツを取得してもよい。

【0572】

(32) 上記の実施の形態では、利用状況テーブルを記録媒体に備えたが、これに限定されない。再生装置に利用状況テーブルを備えてもよい。

【0573】

(33) ライセンスチケットテーブルを用いた残額管理をコンテンツ提供者側にて行つてもよい。

【0574】

このときの実現方法の一例を以下に示す。

【0575】

ライセンスチケット生成装置にて、ライセンスチケットテーブル毎に異なるID（以下

、「ライセンスチケットID」という。)を付与し、ライセンスチケットテーブルにライセンスチケットIDを対応付けて管理する。利用者は、ライセンスチケットを使用する度に、ライセンスチケットIDと、使用したチケット番号とをライセンスチケット生成装置へ送信する。ライセンスチケット生成装置は、受信したライセンスチケットIDとチケット番号とを用いて、利用されたライセンスチケットに対して、利用済の旨の情報を付加する。利用者は、携帯電話機を利用して、ライセンスチケットIDをライセンスチケット生成装置へ送信する。ライセンスチケット生成装置は、ライセンスチケットIDを受信すると、受信したライセンスチケットIDに対応するライセンスチケットテーブルより未使用であるライセンスチケットに係る情報を取得し、取得した情報を用いて残額情報を生成し、生成した残額情報を携帯電話機へ送信する。ここで、残額情報とは、利用できるレンタル回数を示す情報である。携帯電話機は、残額情報を受信すると、受信した残額情報を表示する。

【0576】

なお、残額情報は、利用できるレンタル回数を金額に換算した情報であってもよい。また、残額情報の確認時に利用する装置は、携帯電話機に限らず、上記(4)にて記述した端末装置であってもよい。また、ライセンスチケットIDは、記録媒体に固有の情報であってもよい。記録媒体に固有の情報は、例えば、上記(8)にて示したように、記録媒体に固有のID、BCA領域に記録されている情報、Disc毎又はロット毎に異なるDisc鍵、Disc毎に異なるWobbleから得られるデータである。

【0577】

また、残額管理を行う装置は、ライセンスチケット生成装置に限定されない。残額管理を行う残額管理装置を備えてもよいし、コンテンツ提供装置にて残額管理を行ってもよい。

【0578】

これにより、ライセンスチケットテーブルを用いた残額管理をコンテンツ提供者側にて行うことができる。

【0579】

(34) ライセンスチケット生成装置にて、全ての記録媒体に同一の内容のライセンスチケットテーブルを書き込んだが、これに限定されない。記録媒体毎に、チケット用暗号化マスタ鍵の内容が異なるライセンスチケットテーブルを書き込んでもよい。

【0580】

例えば、第1の実施の形態において、ある記録媒体に書き込むチケット用暗号化マスタ鍵をEnc(DK、WK)とすると、別の記録媒体に書き込むチケット用暗号化マスタ鍵をEnc(DK、WK1)とする。また、例えば、第2の実施の形態において、ある記録媒体に書き込むチケット用暗号化マスタ鍵をEnc(DK、WK1)、Enc(DK、WK2)、・・・、Enc(DK、WK10)とすると、別の記録媒体に書き込むチケット用暗号化マスタ鍵をEnc(DK、WK11)、Enc(DK、WK12)、・・・、Enc(DK、WK20)とする。

【0581】

なお、第3の実施の形態においては、記録媒体毎に、チケット用暗号化マスタ鍵セットの内容が異なるライセンスチケットテーブルを書き込むこととなり、この場合、ある記録媒体に書き込むチケット用暗号化マスタ鍵セットをEnc(DK、WKS1)、Enc(DK、WKS2)、・・・、Enc(DK、WKS10)とすると、別の記録媒体に書き込むチケット用暗号化マスタ鍵をEnc(DK、WKS11)、Enc(DK、WKS12)、・・・、Enc(DK、WKS20)とする。

【0582】

このようにして、記録媒体毎に、異なる内容のライセンスチケットテーブルを書き込むことができる。

【0583】

(35) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピ

ュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0584】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0585】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

【0586】

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであつて、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0587】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0588】

(36) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【0589】

上記において説明したプリペイドカードシステムは、コンテンツ提供者から利用者に対して、映画、音楽などのデジタル化された著作物を供給する産業において、経営的、つまり反復的かつ継続的に利用されうる。特に、デジタル化された著作物をネットワークを介して供給する産業において好適である。

【図面の簡単な説明】

【0590】

【図1】プリペイドカードシステム1を示すブロック図である。

【図2】記録媒体100の構成を示すブロック図である。

【図3】ライセンスチケット記憶部110が有するライセンスチケットテーブルT100のデータ構造を示す。

【図4】コンテンツ記憶部130の構成を示すブロック図である。

【図5】利用状況記憶部140が有する利用状況テーブルT150のデータ構造を示す。

【図6】取得可能コンテンツ一覧画面M100の構成を示す。

【図7】利用形態選択画面M150の構成を示す。

【図8】レンタル用チケット選択画面M200の構成を示す。

【図9】購入用チケット選択画面M250の構成を示す。

【図10】配信要求プログラムを示す流れ図である。図11へ続く。

【図11】配信要求プログラムを示す流れ図である。図10から続く。

【図12】配信要求プログラム内の取得可能コンテンツ一覧生成処理を示す流れ図である。

【図13】配信要求プログラム内の選択コンテンツ受付処理を示す流れ図である。

【図14】配信要求プログラム内の利用形態受付処理を示す流れ図である。

【図15】配信要求プログラム内のレンタル用使用チケット受付処理を示す流れ図である。

【図16】配信要求プログラム内の購入用使用チケット受付処理を示す流れ図である

- 【図17】配信要求プログラム内の購入処理を示す流れ図である。
- 【図18】配信要求プログラム内の利用状況更新処理を示す流れ図である。
- 【図19】再生装置200の構成を示すブロック図である。
- 【図20】再生可能コンテンツ一覧画面M300の構成を示す。
- 【図21】ライセンスチケット生成装置300の構成を示すブロック図である。
- 【図22】コンテンツ提供装置400の構成を示すブロック図である。
- 【図23】コンテンツ関連情報記憶部403が有するコンテンツ関連情報テーブルT400のデータ構造を示す。
- 【図24】配信データ記憶部404が有する暗号化コンテンツ管理テーブルT410のデータ構造を示す。
- 【図25】ライセンスチケット生成時の動作概要を示す流れ図である。
- 【図26】コンテンツ配信要求時の動作概要を示す流れ図である。
- 【図27】ライセンスチケット生成処理の動作を示す流れ図である。
- 【図28】コンテンツ取得処理の動作を示す流れ図である。
- 【図29】再生処理の動作を示す流れ図である。
- 【図30】利用状態確認処理の動作を示す流れ図である。
- 【図31】暗号化コンテンツ生成処理の動作を示す流れ図である。
- 【図32】プリペイドカードシステム2の構成を示すブロック図である。
- 【図33】記録媒体100Aの構成を示すブロック図である。
- 【図34】ライセンスチケット記憶部110Aが有するライセンスチケットテーブルT100Aのデータ構造を示す。
- 【図35】レンタルコンテンツ記憶部131Aの構成を示すブロック図である。
- 【図36】再生装置200Aの構成を示すブロック図である。
- 【図37】ライセンスチケット生成装置300Aの構成を示すブロック図である。
- 【図38】コンテンツ提供装置400Aの構成を示すブロック図である。
- 【図39】ライセンスチケット変更処理の動作を示す流れ図である。
- 【図40】マスタ鍵無効化処理の動作を示す流れ図である。
- 【図41】プリペイドカードシステム3の構成を示すブロック図である。
- 【図42】木構造による鍵管理を示す図である。
- 【図43】(a) リーフ以外の各ノードに割り当てられたマスタ鍵を示す図である。

【0591】

- (b) リーフに割り当てられた各マスタ鍵セットの有するマスタ鍵を示す図である。

- 【図44】記録媒体100Bの構成を示すブロック図である。
- 【図45】ライセンスチケット記憶部110Bが有するライセンスチケットテーブルT100Bのデータ構造を示す。
- 【図46】レンタルコンテンツ記憶部131Bの構成を示すブロック図である。
- 【図47】再生装置200Bの構成を示すブロック図である。
- 【図48】ライセンスチケット生成装置300Bの構成を示すブロック図である。
- 【図49】コンテンツ提供装置400Bの構成を示すブロック図である。
- 【図50】ライセンスチケット生成処理の動作を示す流れ図である。

【符号の説明】

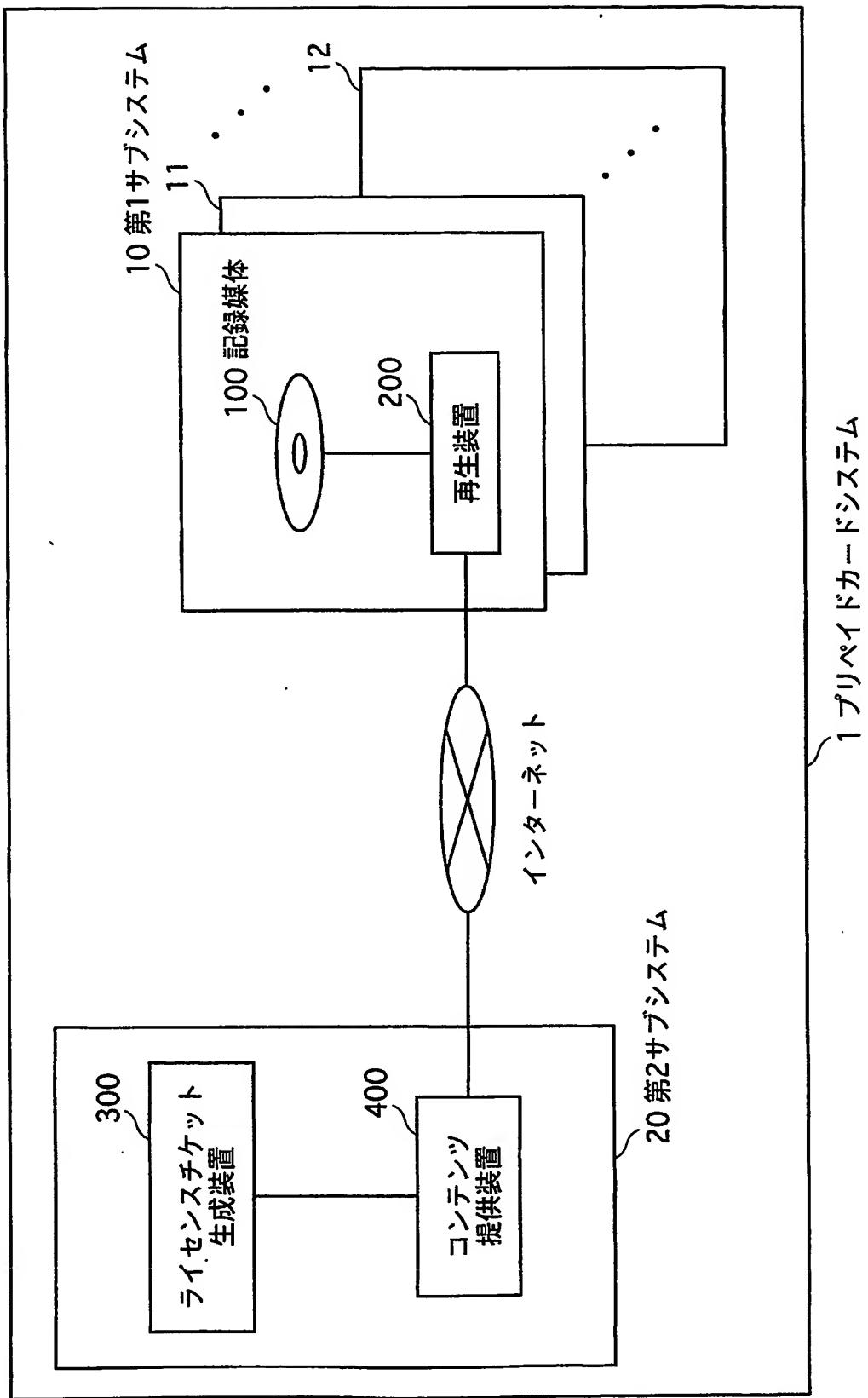
【0592】

- 1 プリペイドカードシステム
- 10～12 第1サブシステム
- 20 第2サブシステム
- 100 記録媒体
- 101 ROM領域

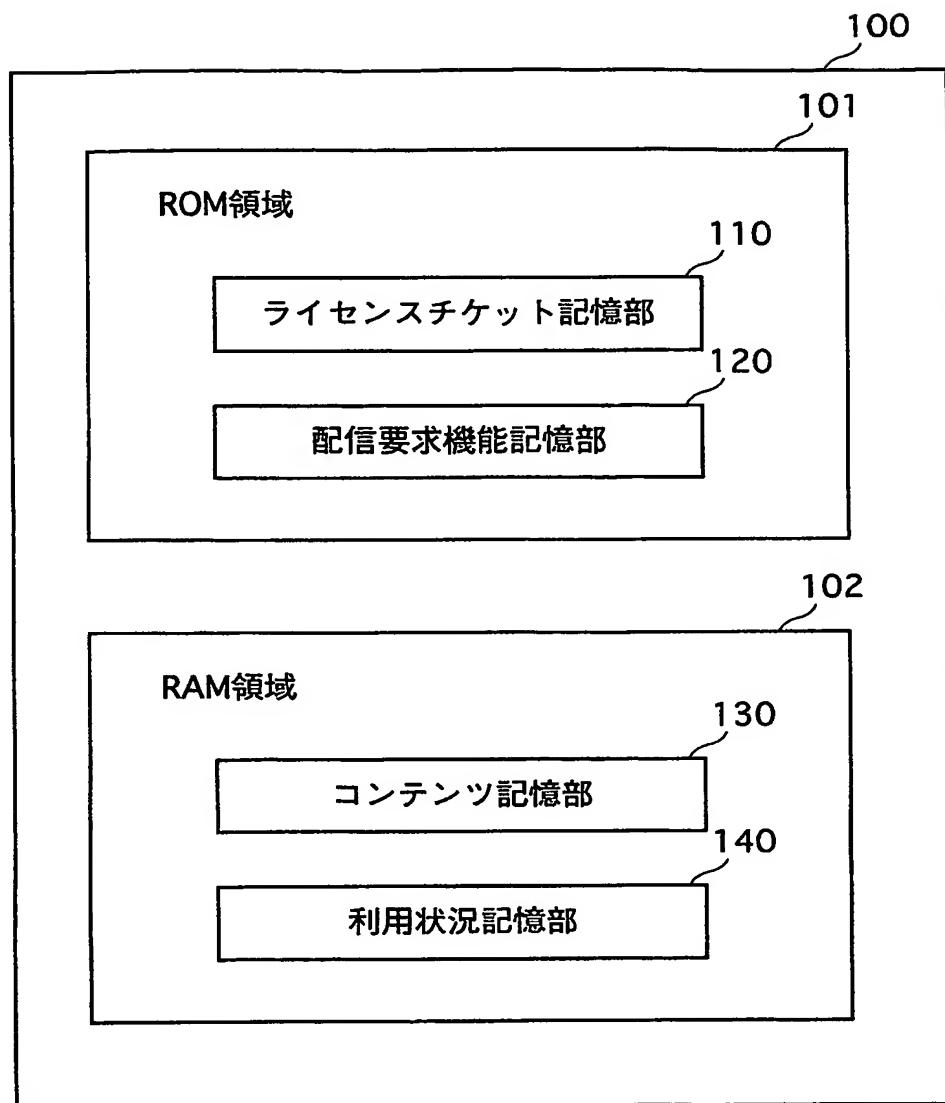
102 RAM領域
110 ライセンスチケット記憶部
120 配信要求機能記憶部
130 コンテンツ記憶部
131 レンタルコンテンツ記憶部
132 購入コンテンツ記憶部
140 利用状況記憶部
200 再生装置
201 デバイス鍵記憶部
202 時計部
203 配信要求処理部
204 再生処理部
205 入力部
206 出力部
207 第1入出力部
208 第2入出力部
210 リモコン
300 ライセンスチケット生成装置
301 デバイス鍵記憶部
302 暗号鍵記憶部
303 マスタ鍵生成部
304 チケット用暗号化部
305 ライセンスチケット生成部
306 書込部
307 出力用暗号化部
308 出力部
309 チケット情報記憶部
400 コンテンツ提供装置
401 復号鍵記憶部
402 マスタ鍵記憶部
403 コンテンツ関連情報記憶部
404 配信データ記憶部
405 受信部
406 復号部
407 入力部
408 コンテンツ鍵生成部
409 暗号化部
410 コンテンツ読込部
411 配信処理部
412 送受信部

【書類名】 図面

【図 1】



【図2】



【図3】

T100

チケット 番号	利用可能 コンテンツID	利用規則		チケット用暗号化 マスタ鍵
		レンタル	購入	
1	100*****	3日	300円	Enc(DK,WK)
2	100*****	3日	300円	Enc(DK,WK)
3	100*****	3日	300円	Enc(DK,WK)
4	100*****	5日	500円	Enc(DK,WK)
5	100*****	5日	500円	Enc(DK,WK)
6	100*****	5日	500円	Enc(DK,WK)
7	100*****	7日	700円	Enc(DK,WK)
8	100*****	7日	700円	Enc(DK,WK)
9	100*****	7日	700円	Enc(DK,WK)
10	100*****	10日	1000円	Enc(DK,WK)

【図4】

130

131 レンタルコンテンツ記憶部

コンテンツID 1000001	暗号化コンテンツ鍵、暗号化コンテンツ Enc(WK,CK1)、Enc(CK1,CNT1)
1000002	Enc(WK,CK2)、Enc(CK2,CNT2)
1000005	Enc(WK,CK5)、Enc(CK5,CNT5)
⋮	⋮

132 購入コンテンツ記憶部

コンテンツID 1000007	コンテンツ CNT7
⋮	⋮

【図5】

T150

利用番号	利用状態	利用形態	利用開始日時	コンテンツID	コンテンツ名	定価
1	利用済	レンタル	2003年5月1日 12:00	1000001	AAA	700円
2	利用済	レンタル	2003年5月15日 20:00	1000002	BBB	700円
3	未利用					
4	利用済	購入	2003年5月10日 22:00	1000007	GGG	1000円
5	利用済	購入	2003年5月10日22:00	1000007	GGG	1000円
6	未利用					
7	利用中	レンタル	2003年5月20日 18:00	1000005	EEE	700円
8	未利用					
9	未利用					
10	未利用					

【図 6】

M100

取得可能コンテンツ一覧			1/20ページ
コンテンツID	コンテンツ名	定価	
1000001	AAA	700円	M101
1000002	BBB	700円	M102
1000003	CCC	1000円	M103
1000004	DDD	700円	
1000005	EEE	700円	

【図 7】

M150

選択されたコンテンツ

M151

コンテンツID	コンテンツ名	定価
1000003	CCC	1000円

利用形態

M152

レンタル

購入

【図8】

M200

ライセンスチケット選択		
コンテンツID	コンテンツ名	定価
1000003	CCC	1000円

M201

M202

チケット番号	利用可能コンテンツID	利用規則(レンタル)
3	100****	3日
6	100****	5日
8	100****	7日
9	100****	7日
10	100****	10日

【図9】

M250

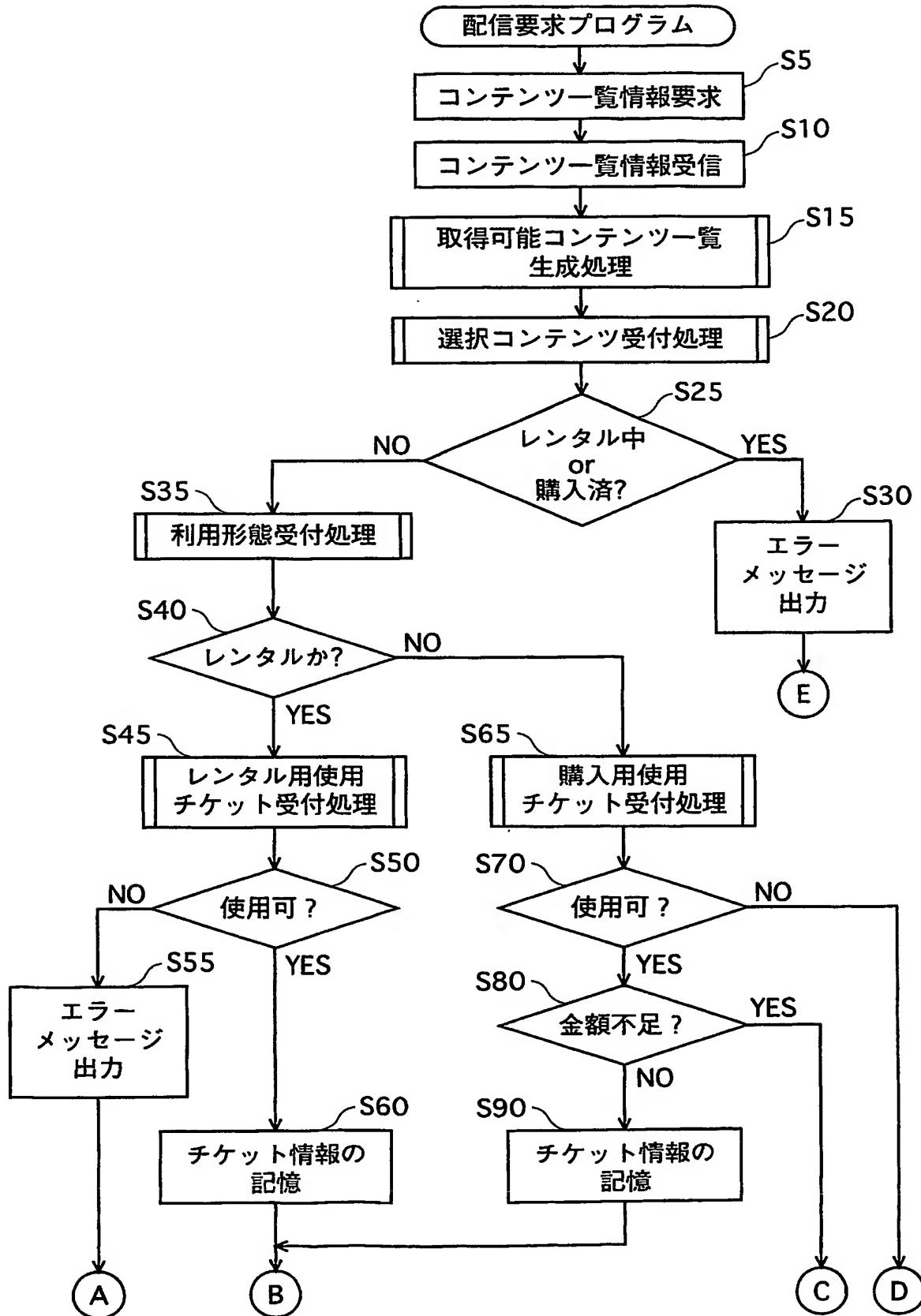
M251

M252

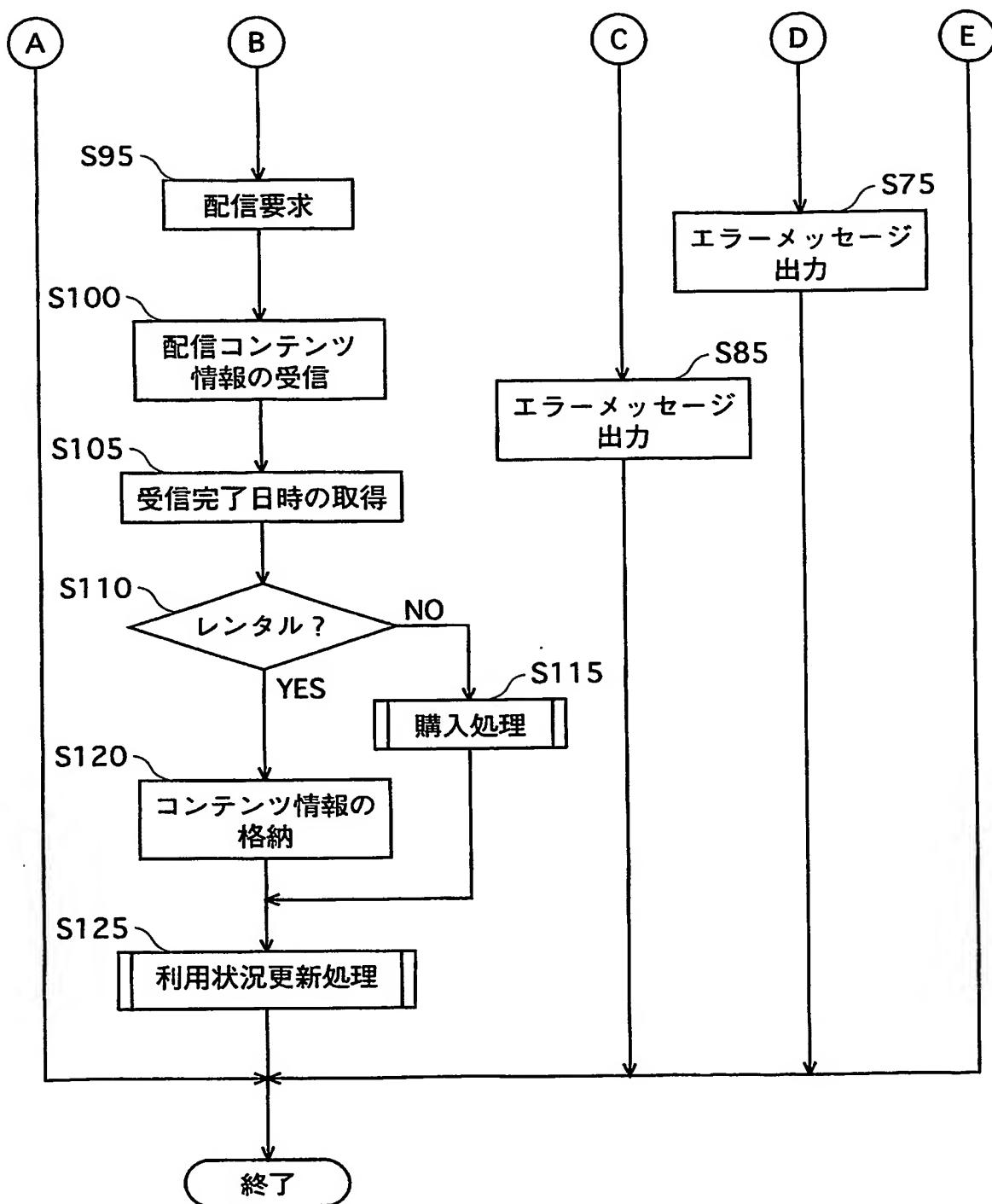
ライセンスチケット選択		
コンテンツID	コンテンツ名	定価
1000003	CCC	1000円

利用可能ライセンスチケット(複数選択可)		
チケット番号	利用可能コンテンツID	利用規則(購入)
3	100*****	300円
6	100*****	500円
8	100*****	700円
9	100*****	700円
10	100*****	1000円

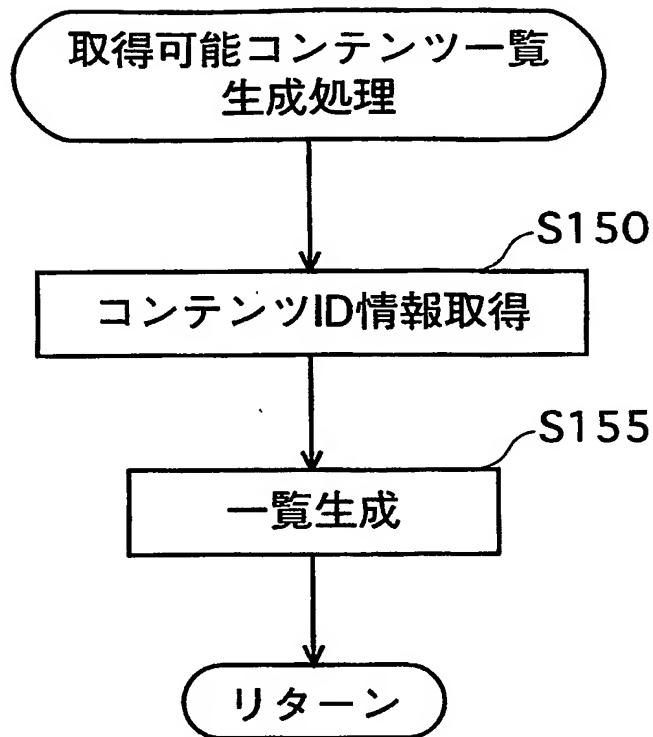
【図10】



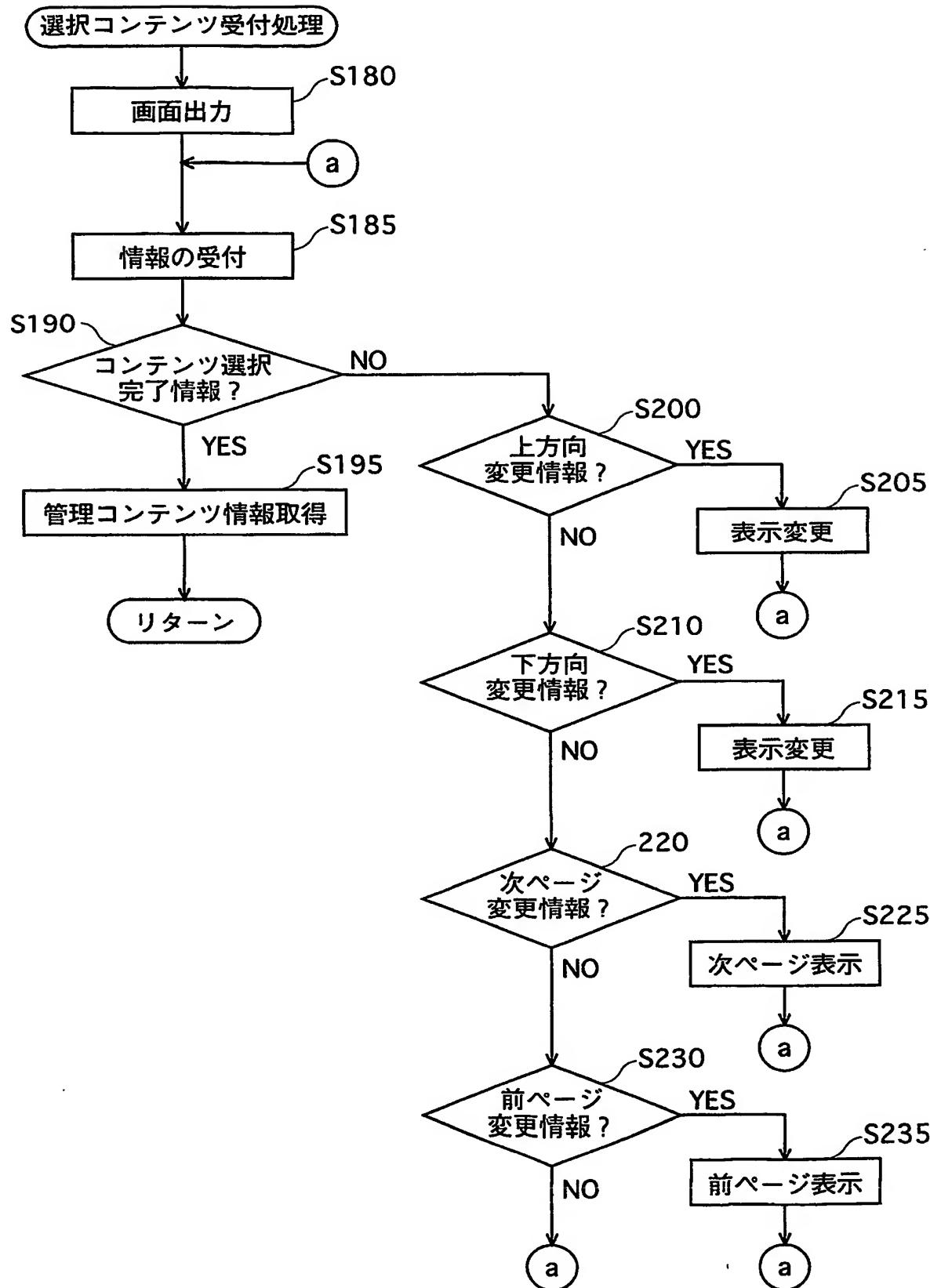
【図11】



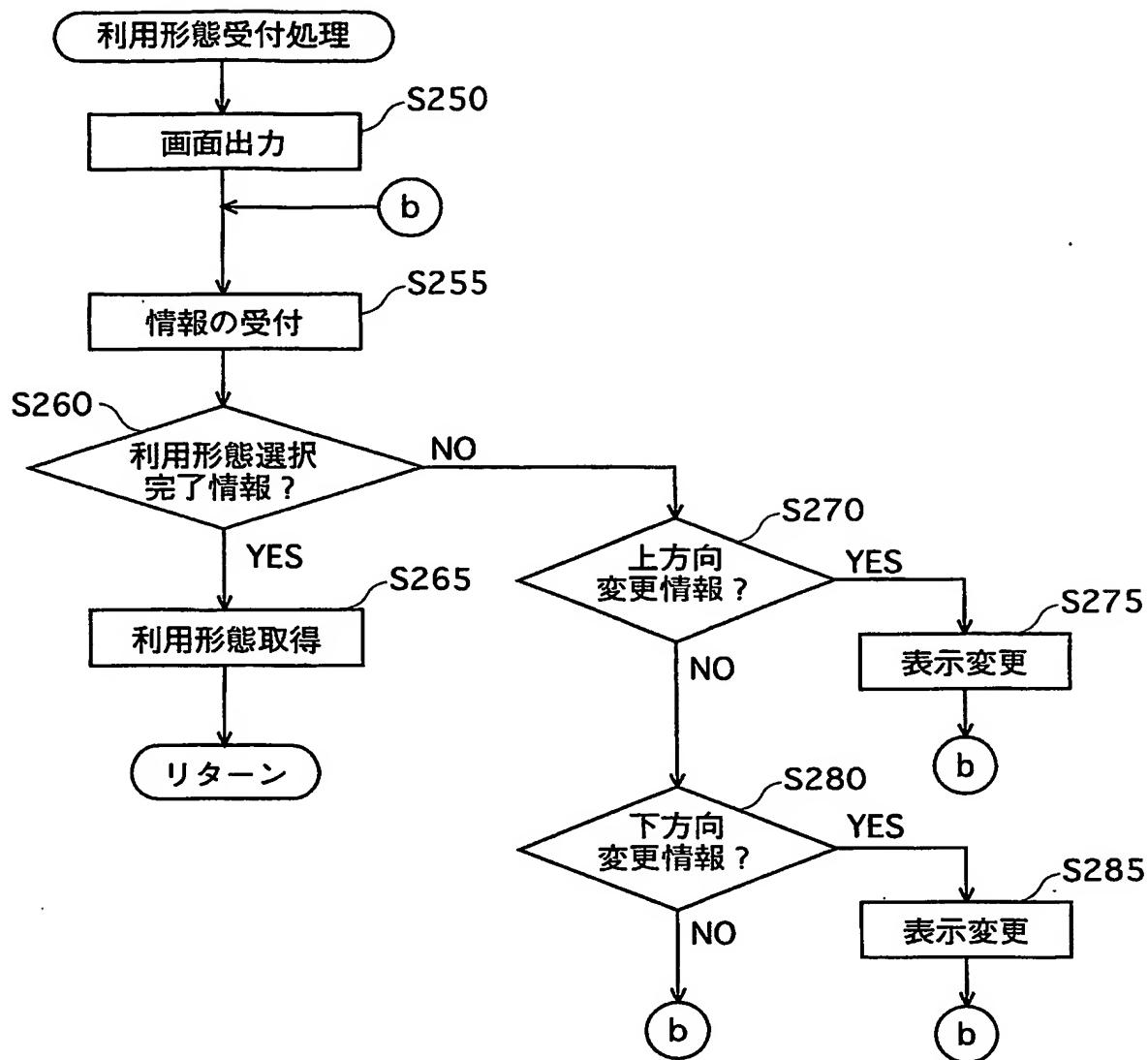
【図12】



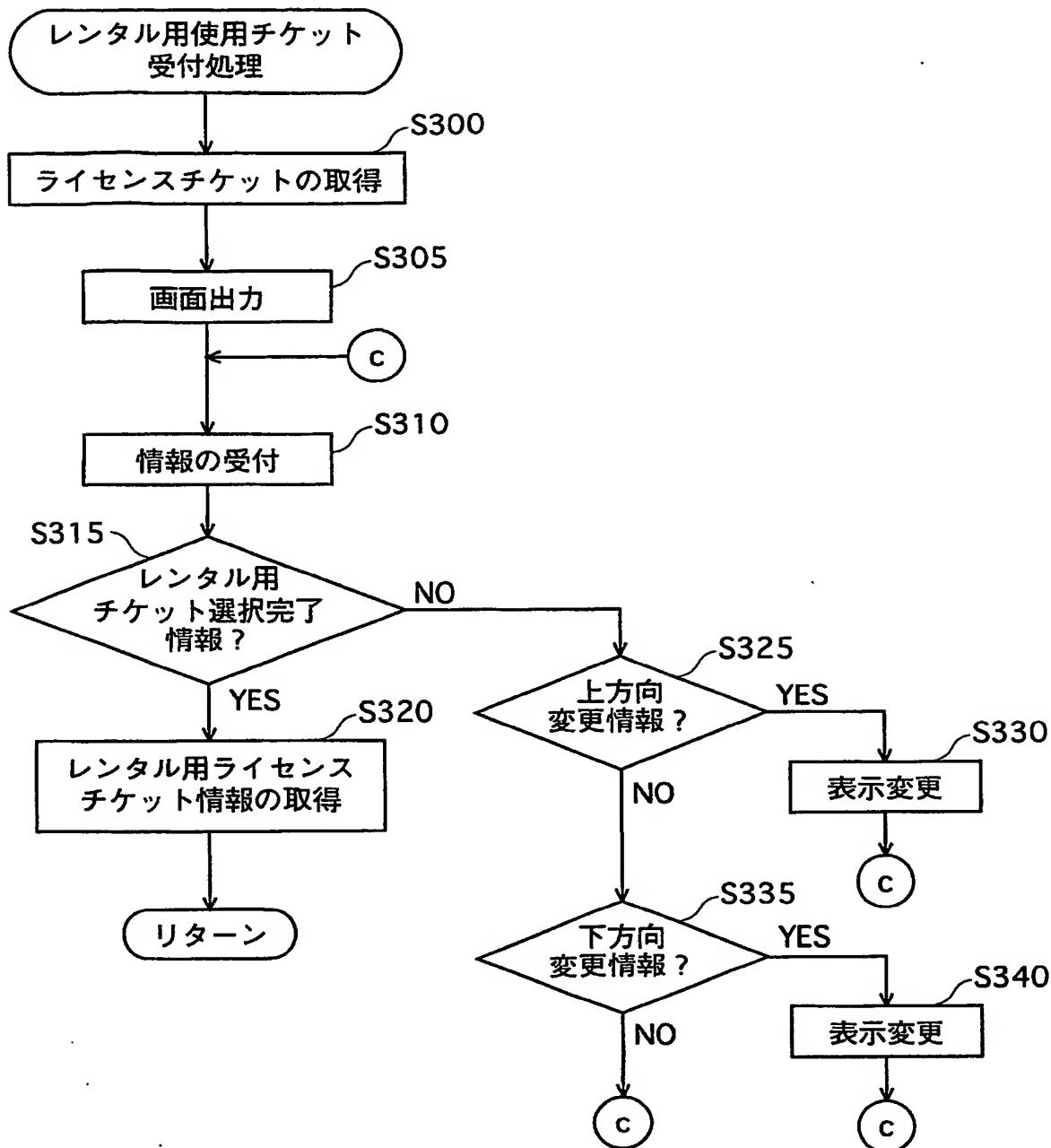
【図13】



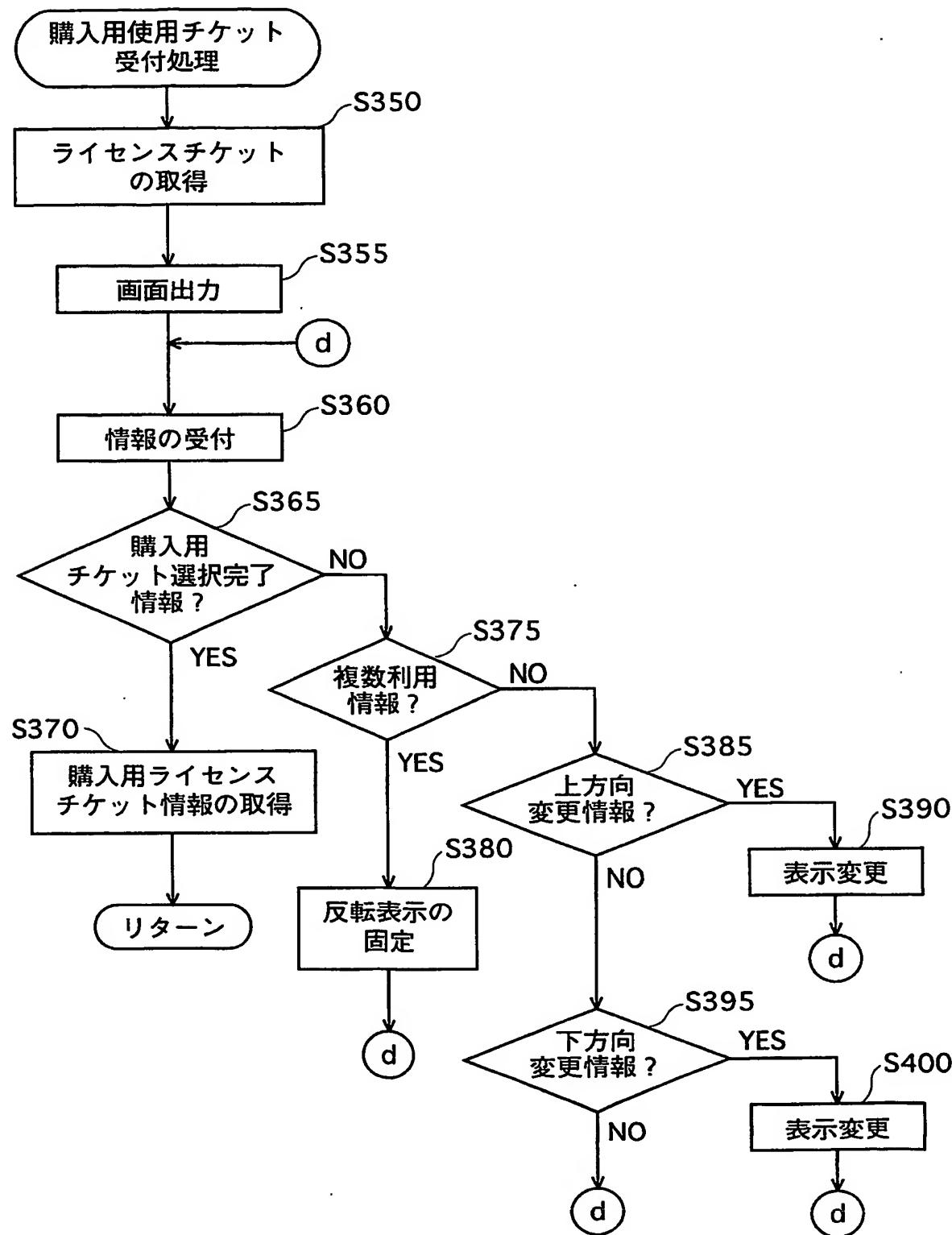
【図14】



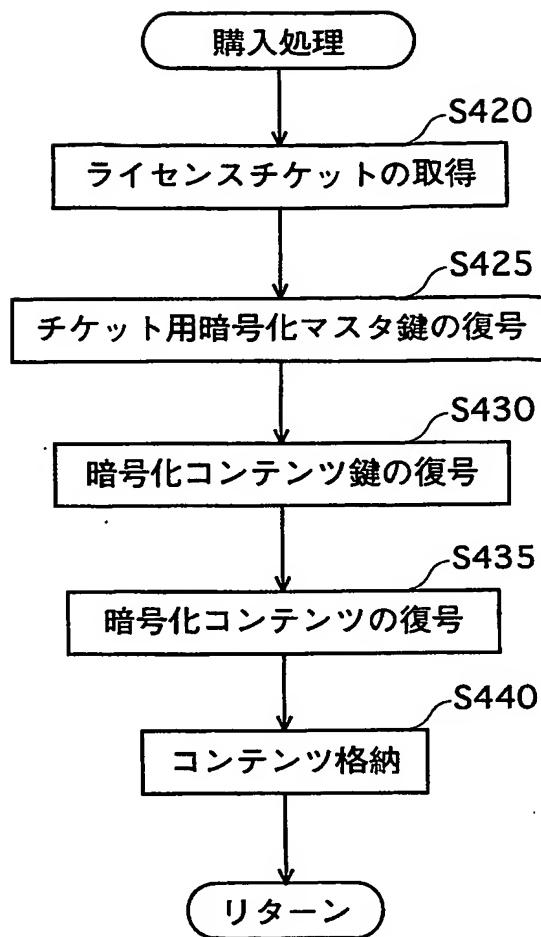
【図 15】



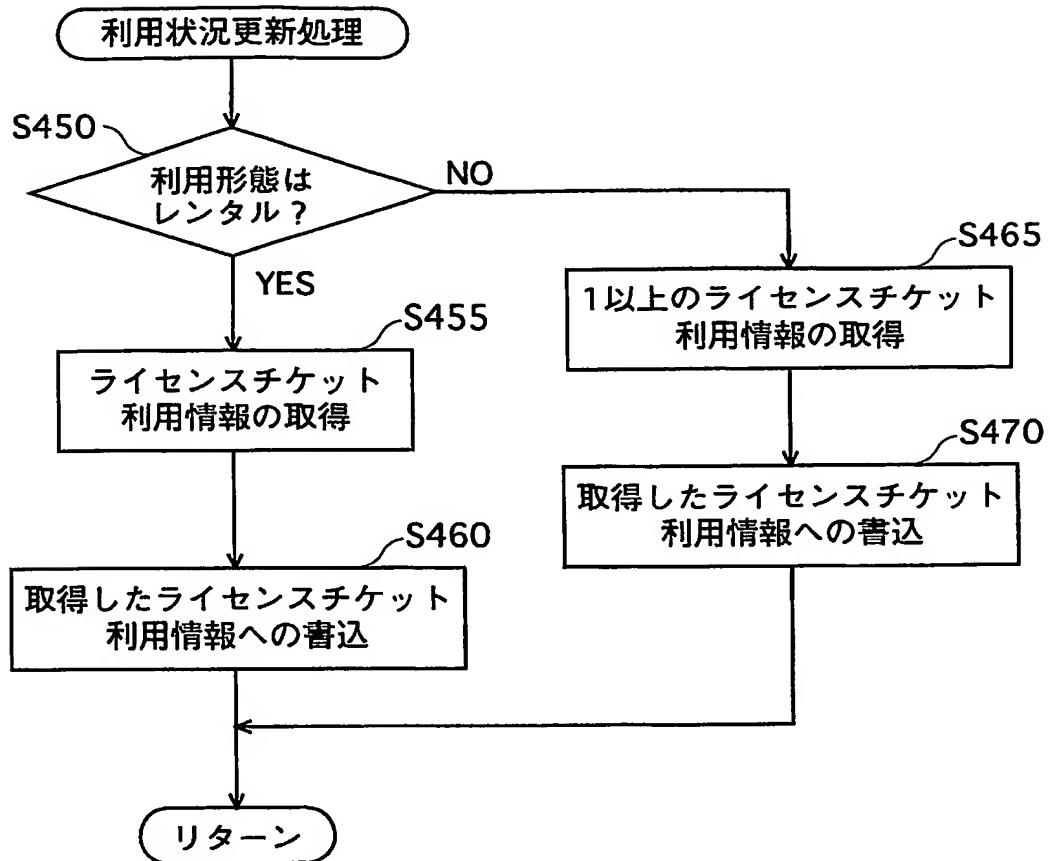
【図16】



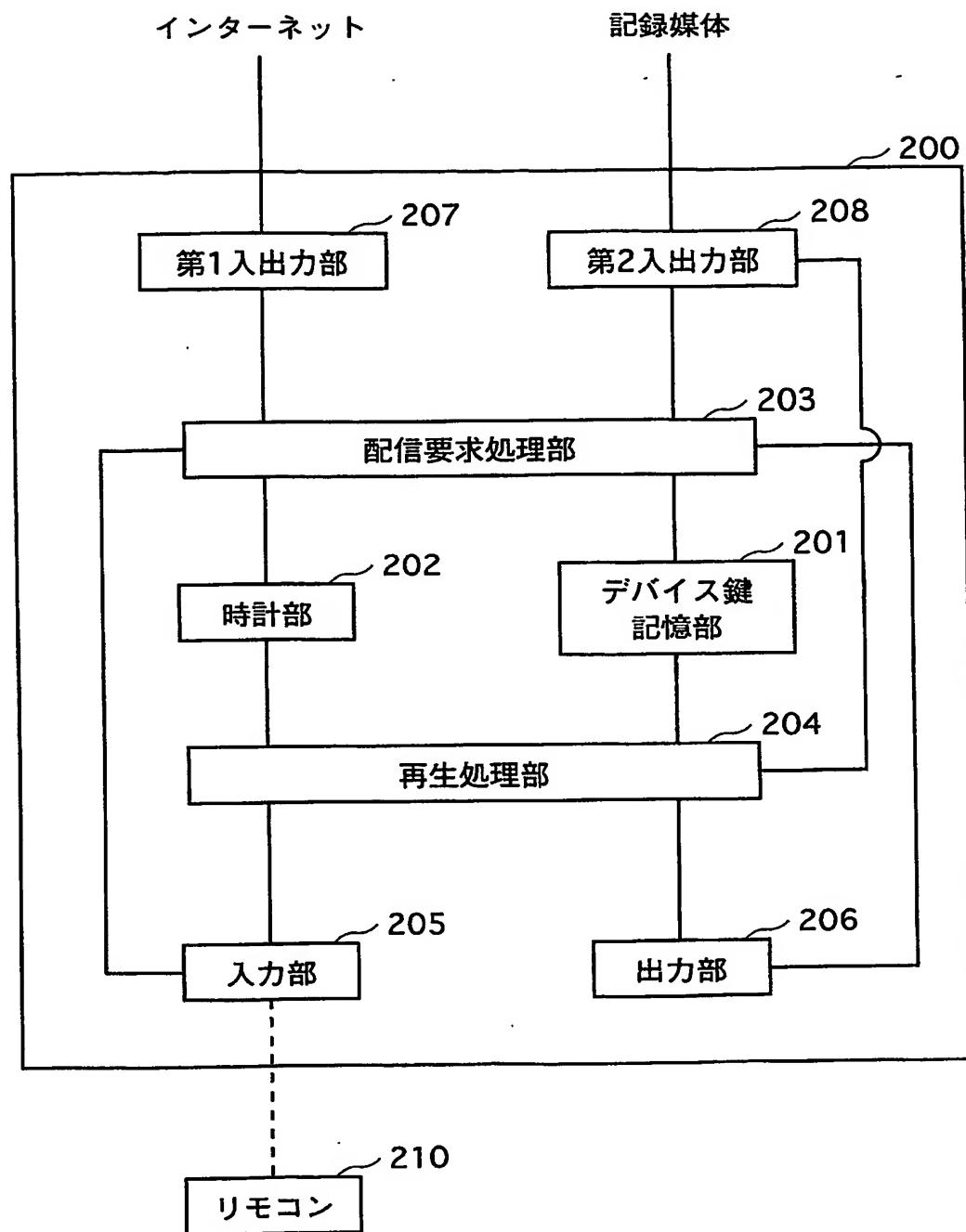
【図17】



【図 18】



【図19】



【図20】

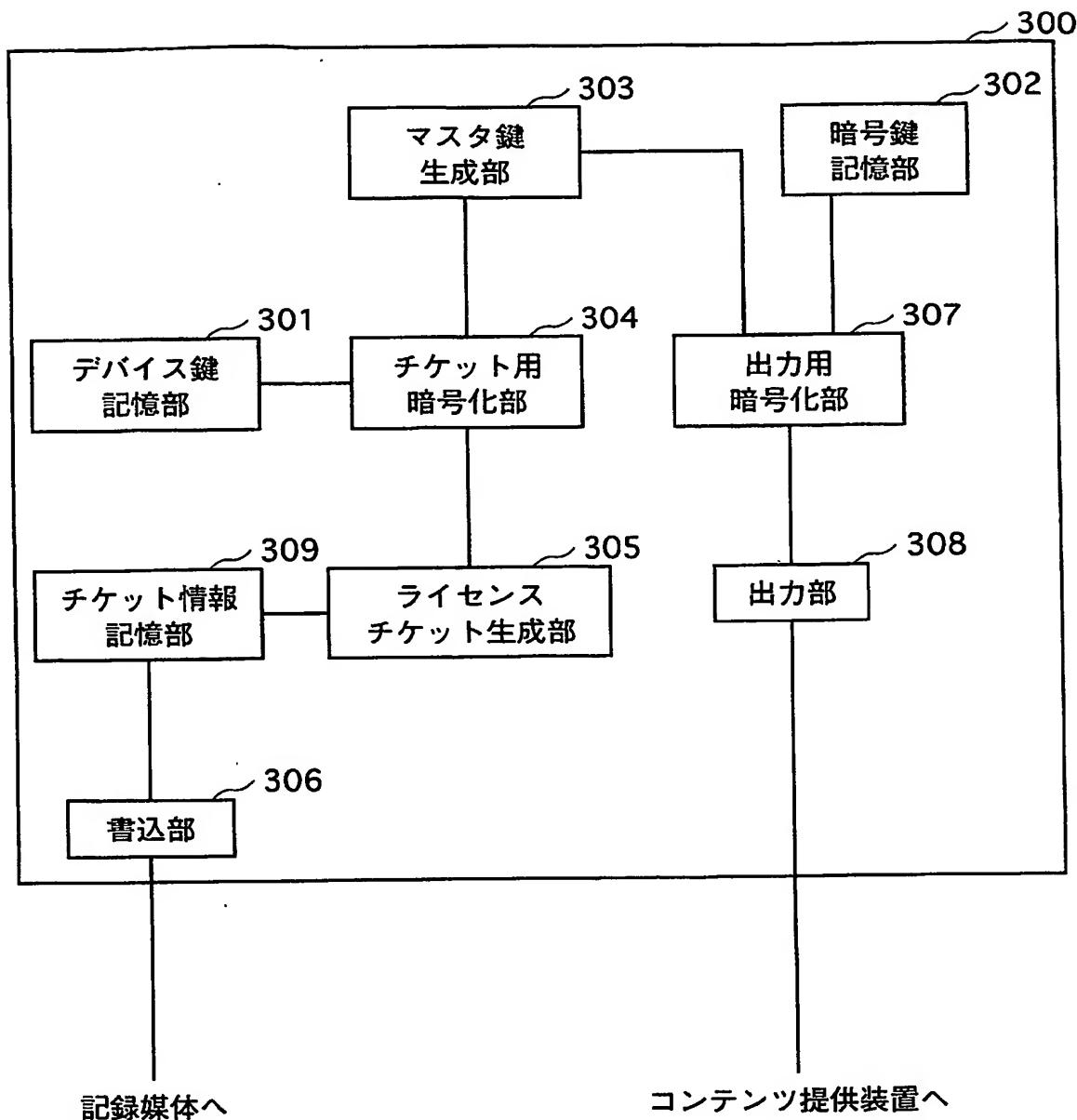
M300

再生コンテンツ選択

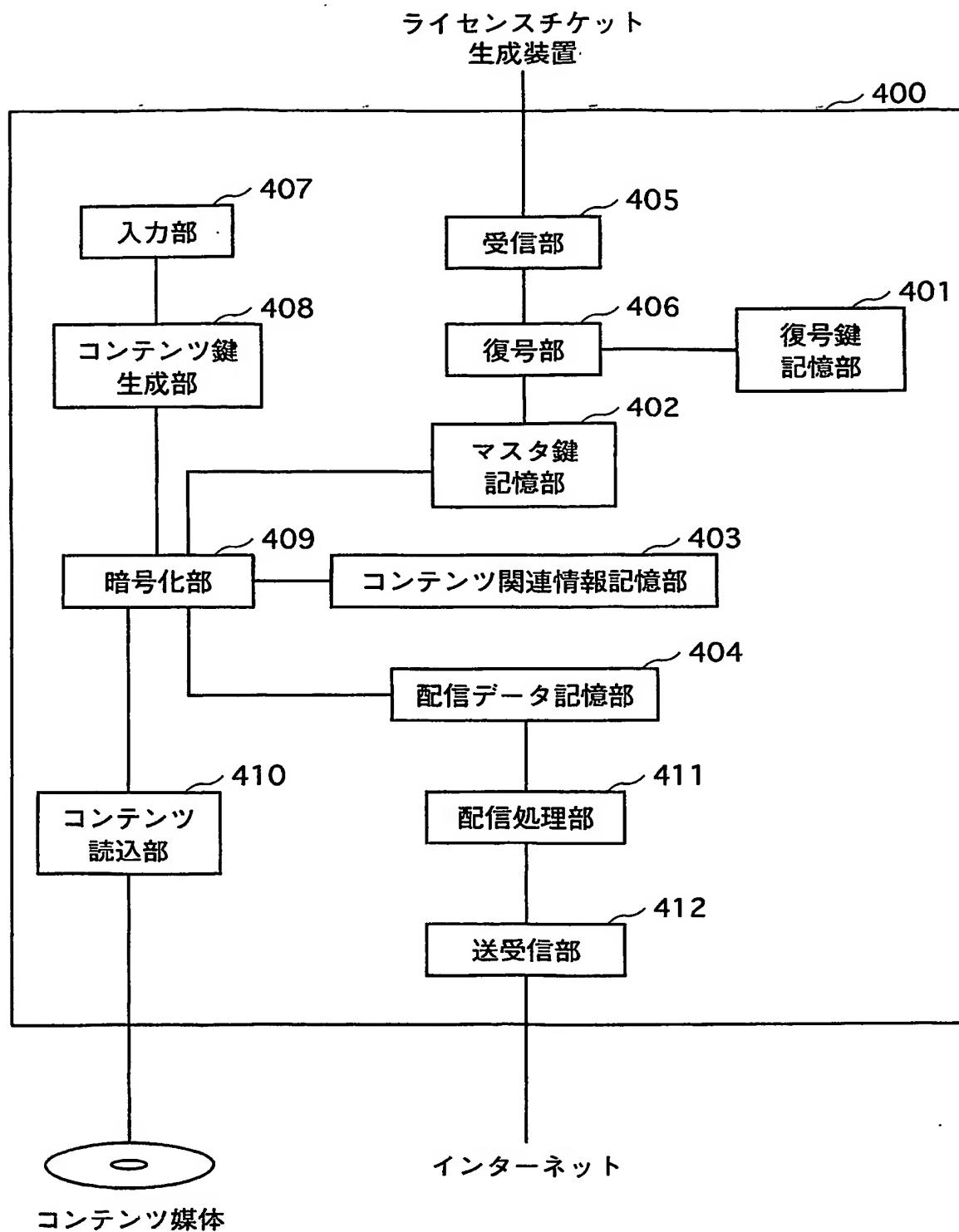
M301

利用番号	コンテンツID	コンテンツ名
4	1000007	GGG
7	1000005	EEE

【図21】



【図 22】



【図23】

↖ T400

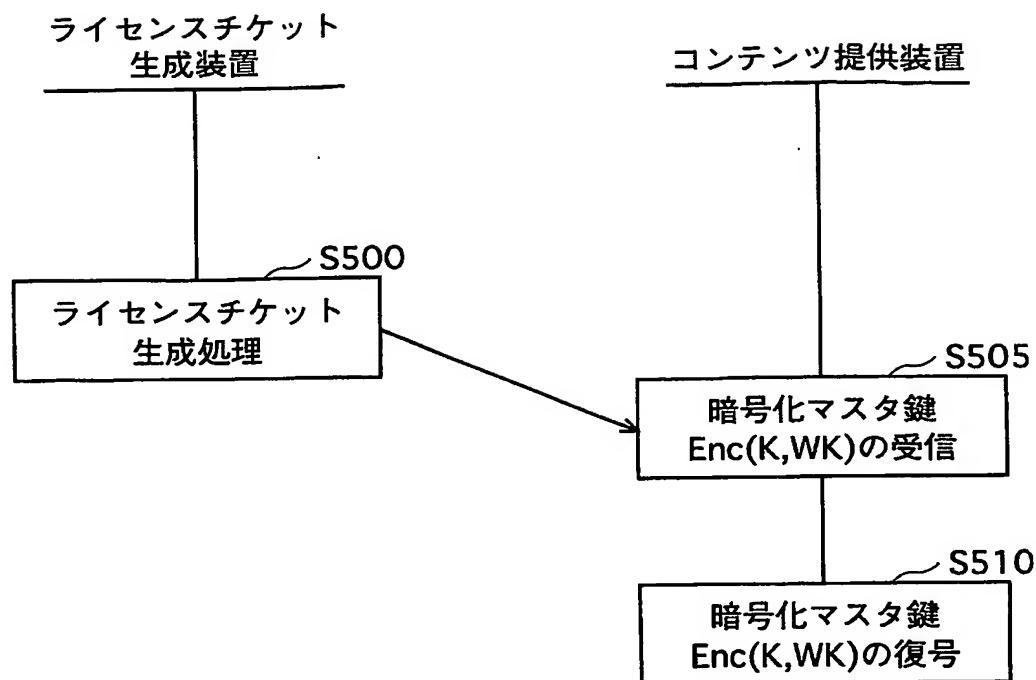
コンテンツID	コンテンツ名	定価
1000001	AAA	700円
1000002	BBB	700円
1000003	CCC	1000円
1000004	DDD	700円
1000005	EEE	700円
⋮	⋮	⋮

【図 24】

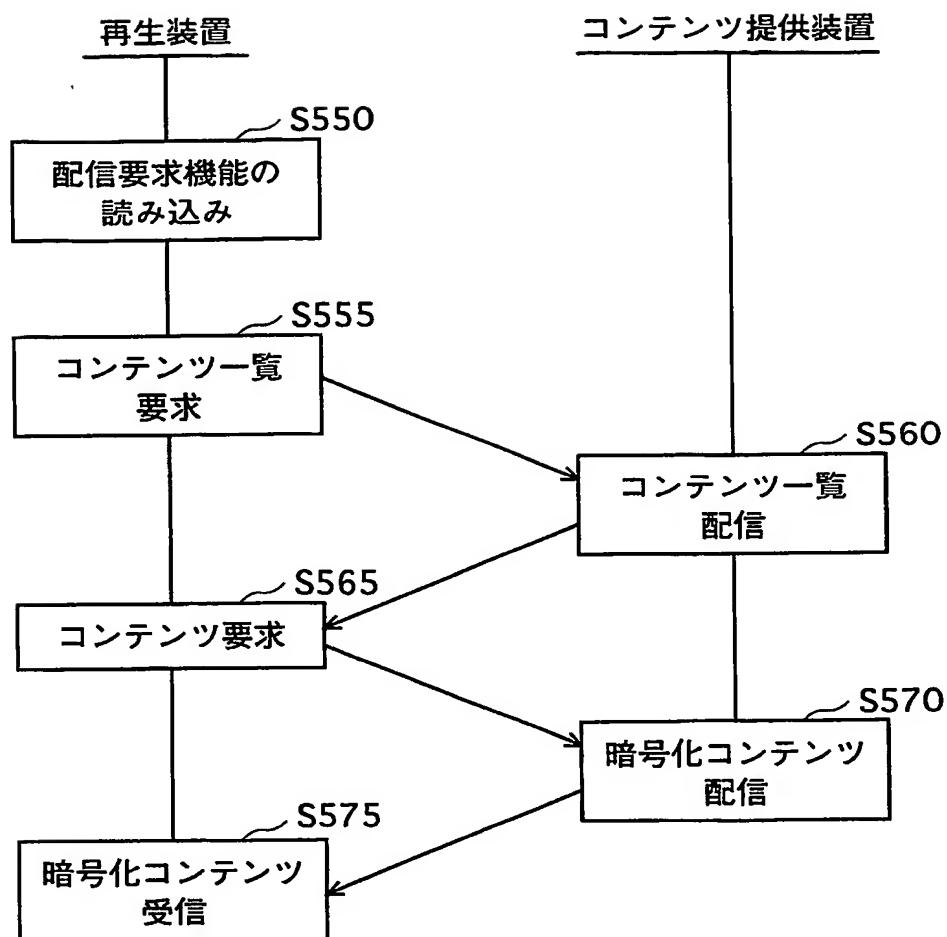
T410

コンテンツID	コンテンツ名	暗号化コンテンツ鍵	暗号化コンテンツ	定価
1000001	AAA	Enc(WK,CK1)	Enc(CK1,CNT1)	700円
1000002	BBB	Enc(WK,CK2)	Enc(CK2,CNT2)	700円
1000003	CCC	Enc(WK,CK3)	Enc(CK3,CNT3)	1000円
1000004	DDD	Enc(WK,CK4)	Enc(CK4,CNT4)	700円
1000005	EEE	Enc(WK,CK5)	Enc(CK5,CNT5)	700円
⋮	⋮	⋮	⋮	⋮

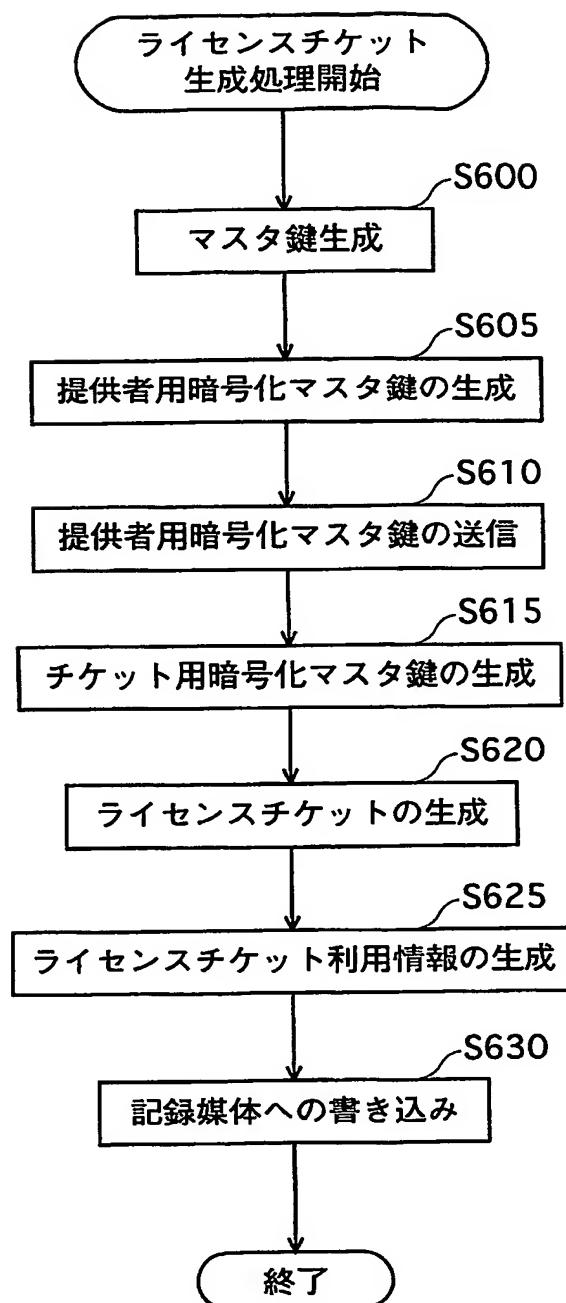
【図 25】



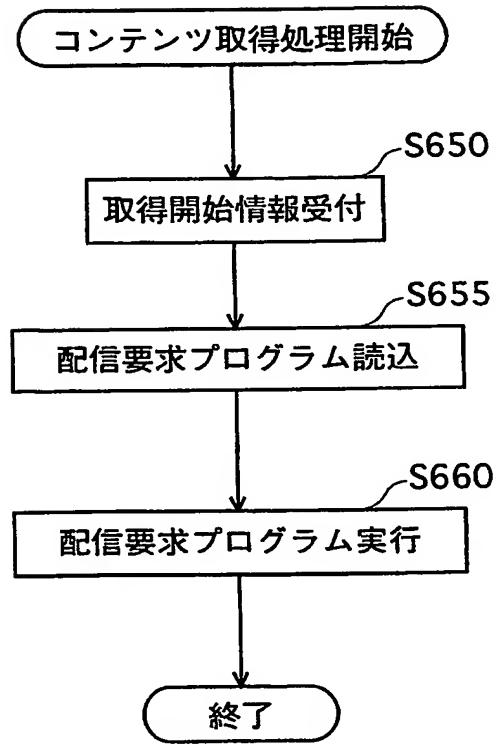
【図26】



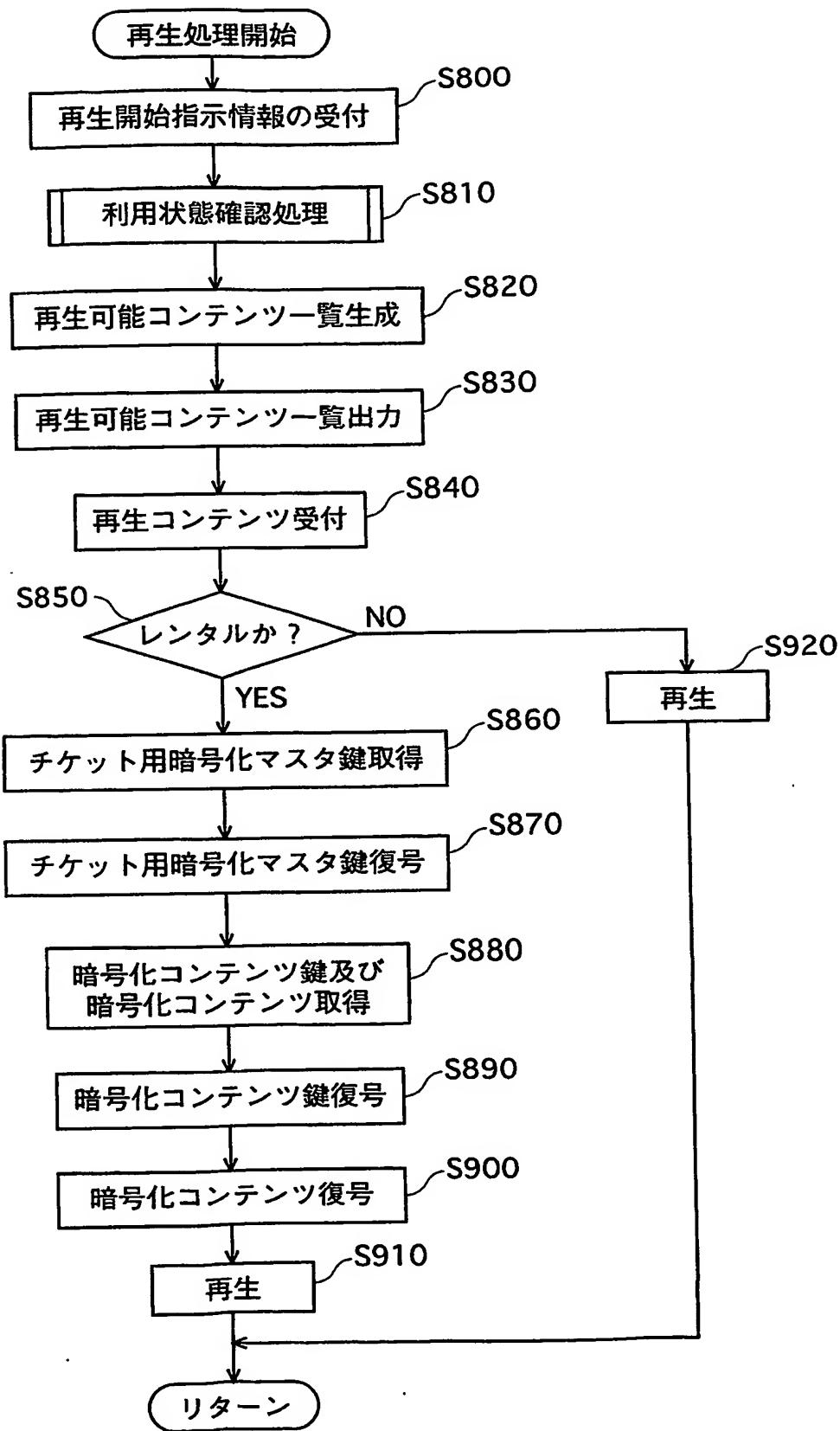
【図27】



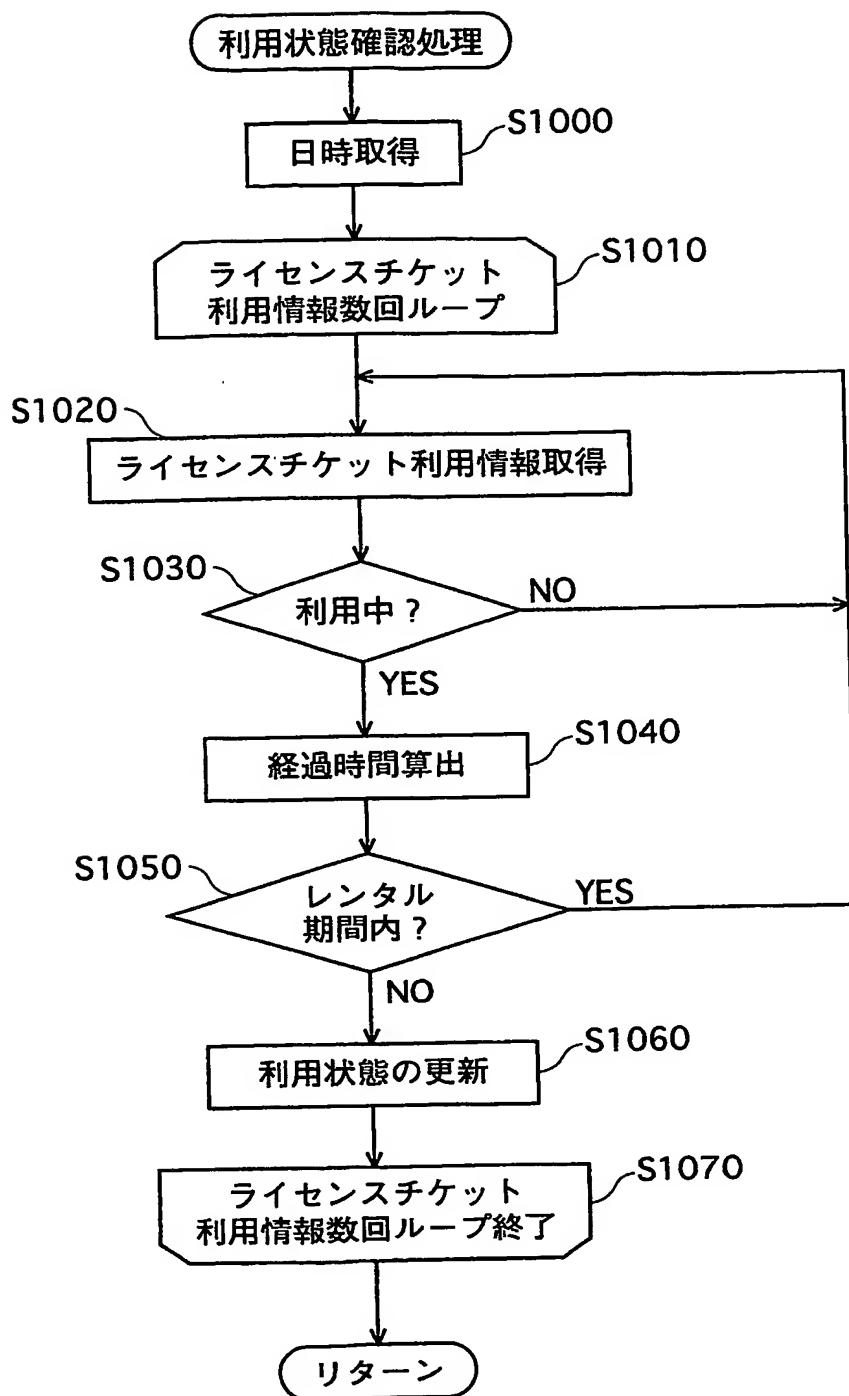
【図28】



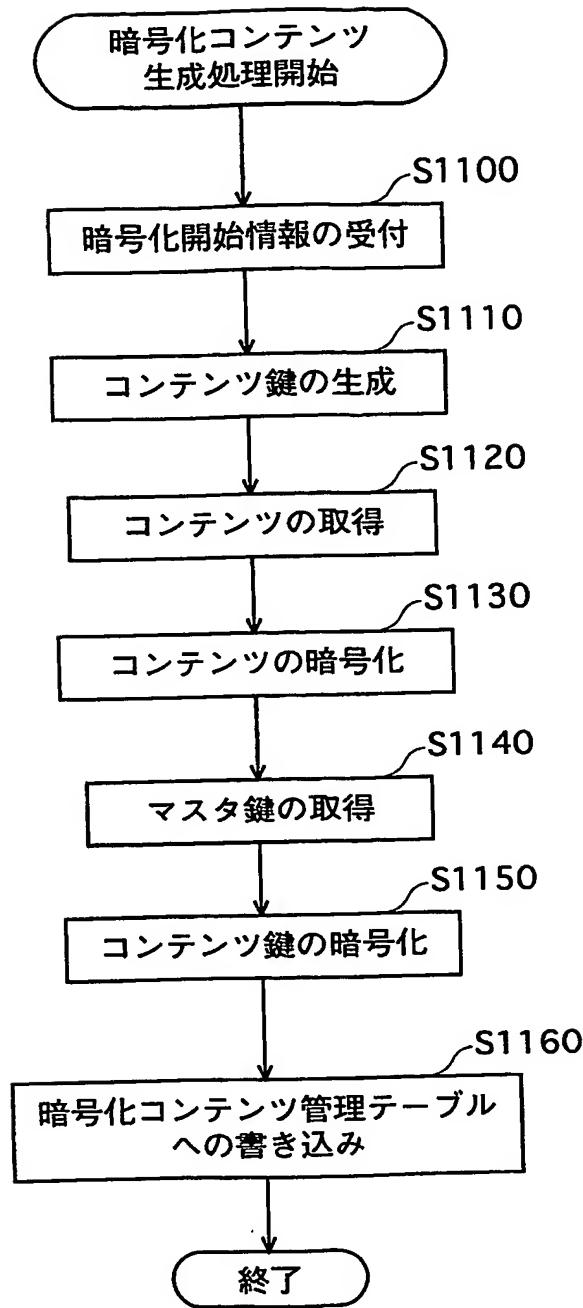
【図29】



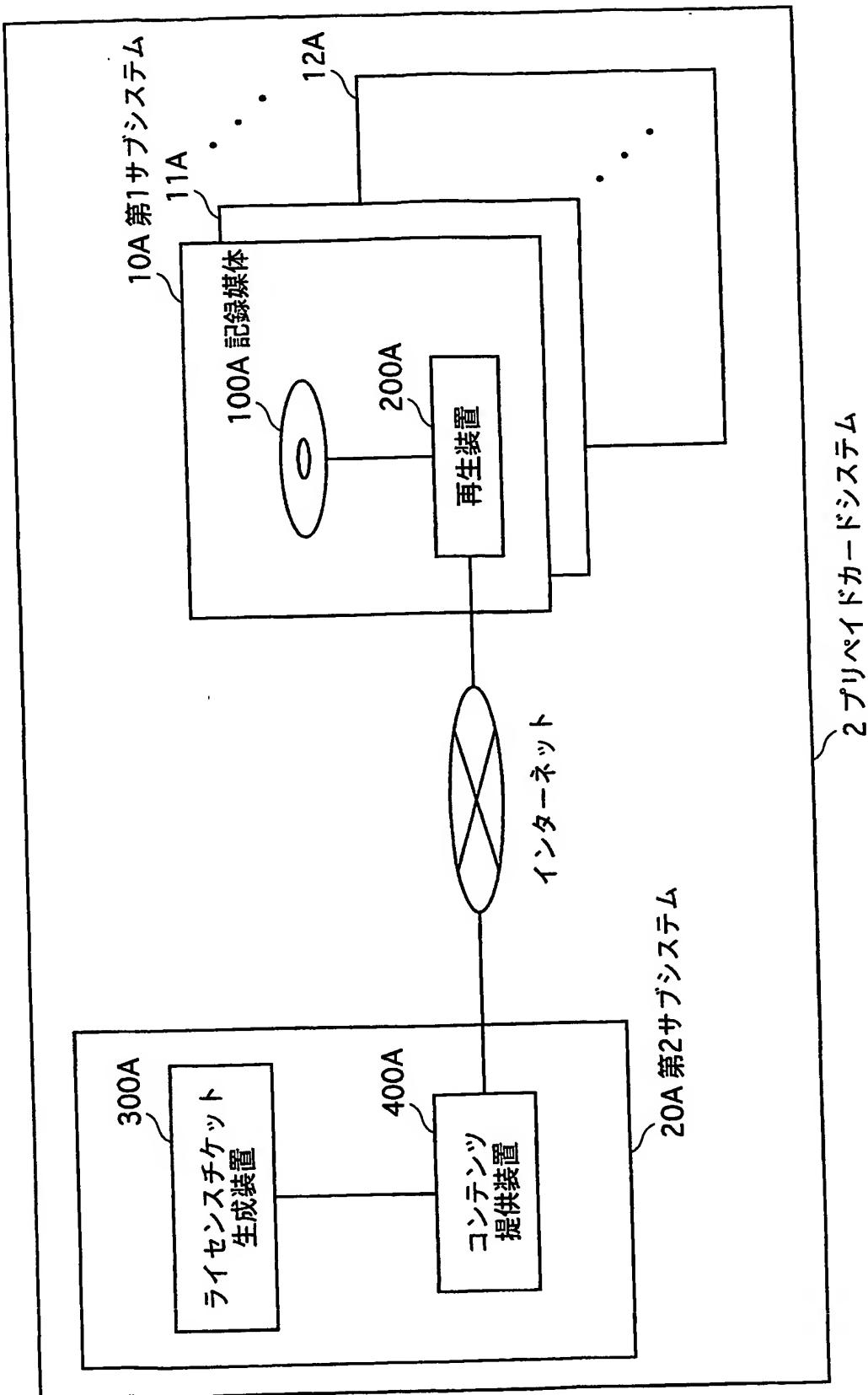
【図30】



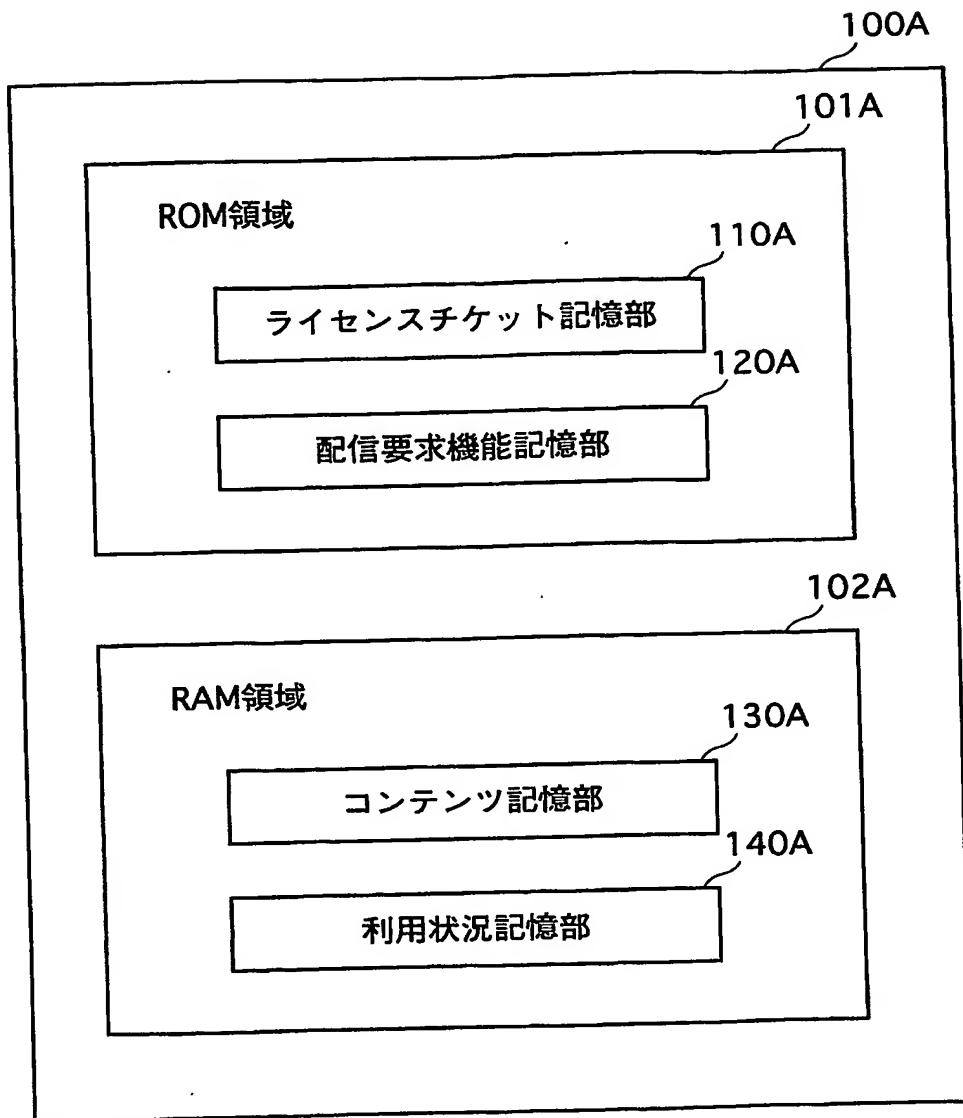
【図31】



【図32】



【図33】



【図34】

T100A

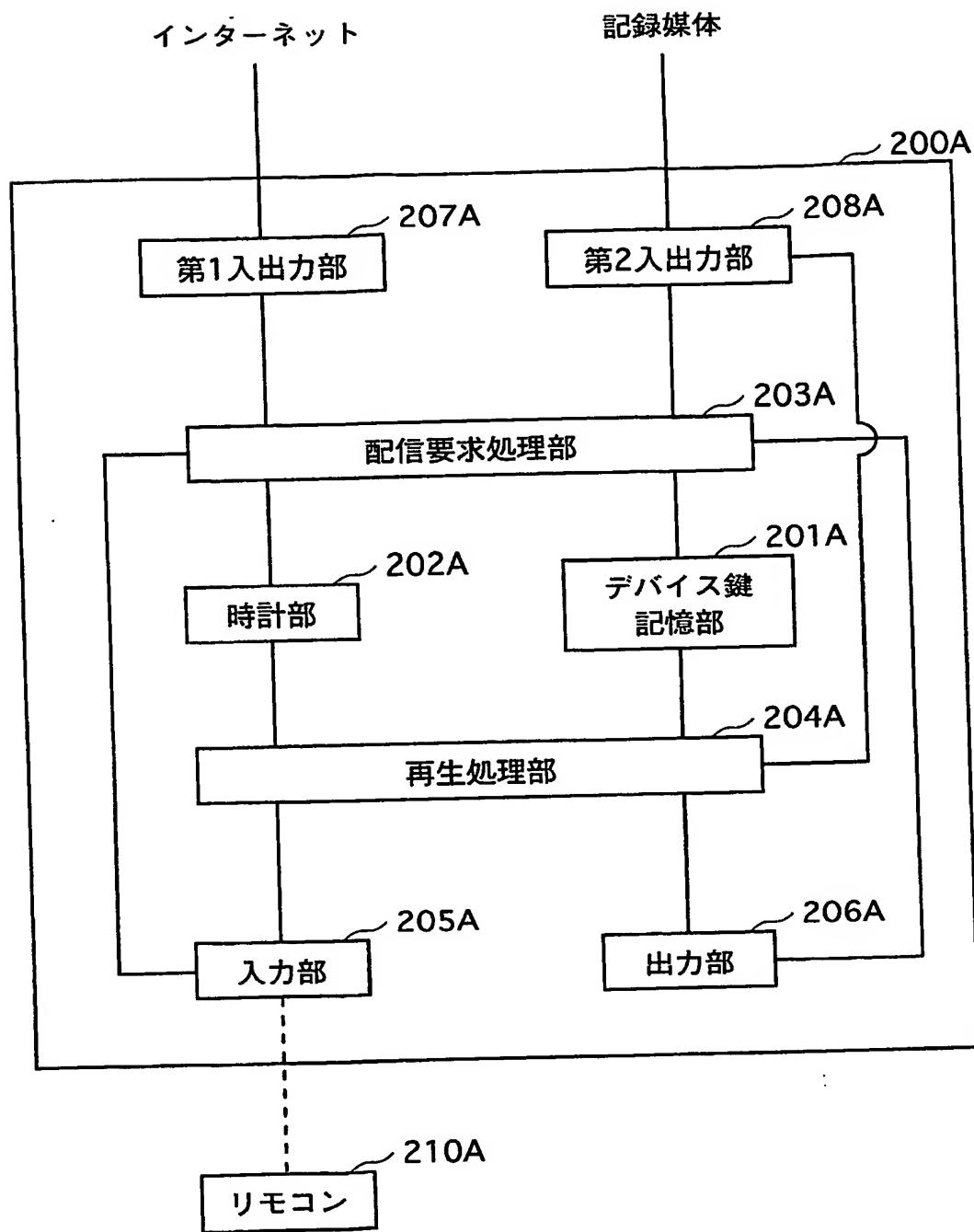
チケット番号	利用可能コンテンツID	利用規則		チケット用暗号化マスタ鍵
		レンタル	購入	
1	100****	3日	300円	Enc(DK,WK1)
2	100****	3日	300円	Enc(DK,WK2)
3	100****	3日	300円	Enc(DK,WK3)
4	100****	5日	500円	Enc(DK,WK4)
5	100****	5日	500円	Enc(DK,WK5)
6	100****	5日	500円	Enc(DK,WK6)
7	100****	7日	700円	Enc(DK,WK7)
8	100****	7日	700円	Enc(DK,WK8)
9	100****	7日	700円	Enc(DK,WK9)
10	100****	10日	1000円	Enc(DK,WK10)

【図 35】

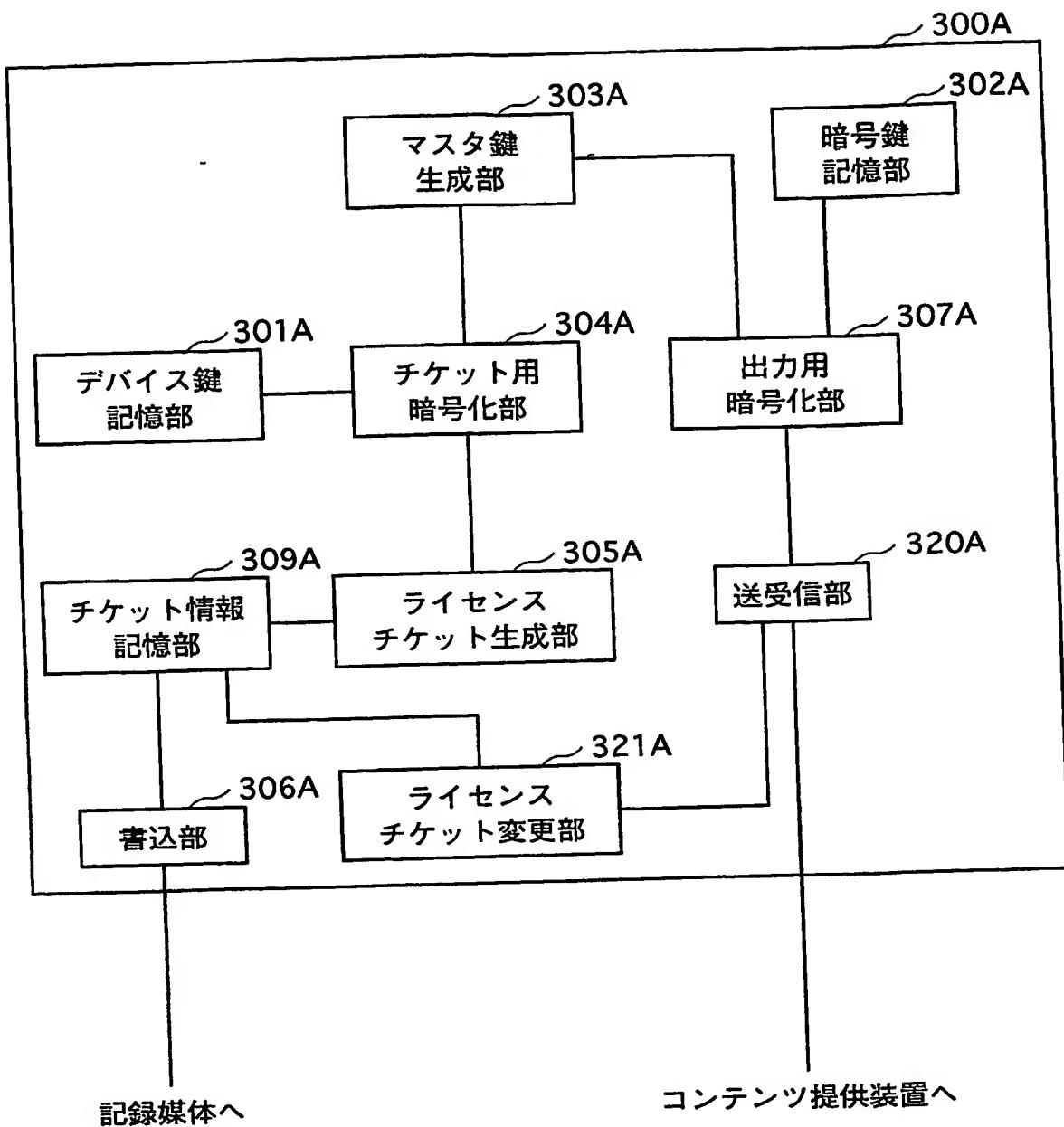
131A

コンテンツID	(インデックス情報、暗号化コンテンツ鍵)	暗号化コンテンツ Enc(CK1,CNT1)
10000001	(1,Enc(WK1,CK1)), (2,Enc(WK2,CK1)), ⋮	
	(10,Enc(WK10,CK1)), ⋮	
10000002	(1,Enc(WK1,CK2)), (2,Enc(WK2,CK2)), ⋮	
	(10,Enc(WK10,CK2)), ⋮	

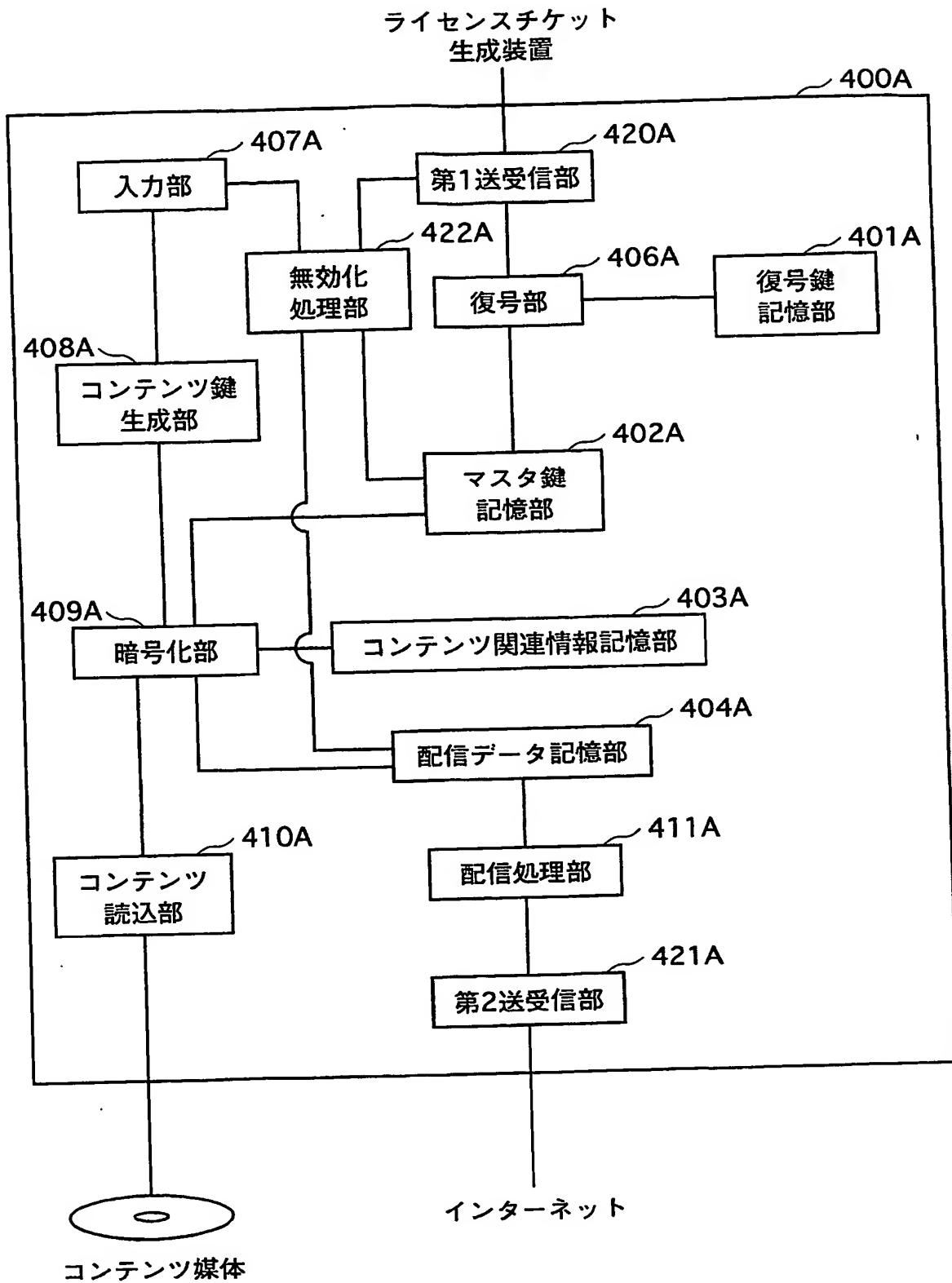
【図36】



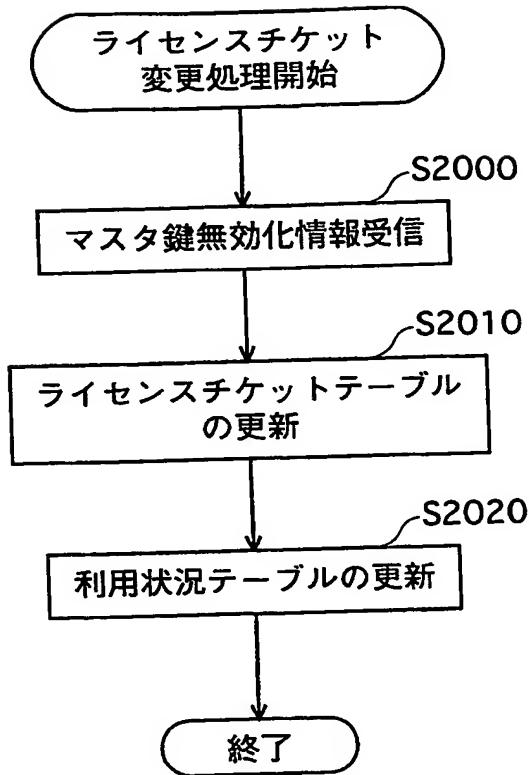
【図 37】



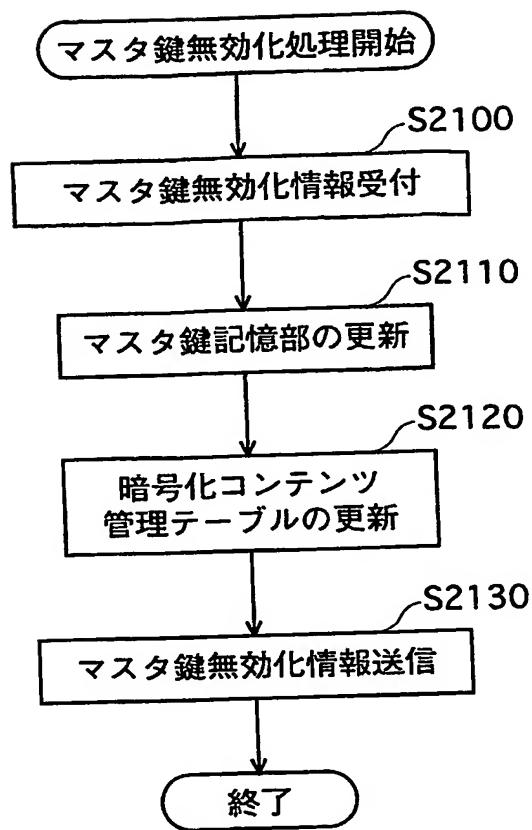
【図38】



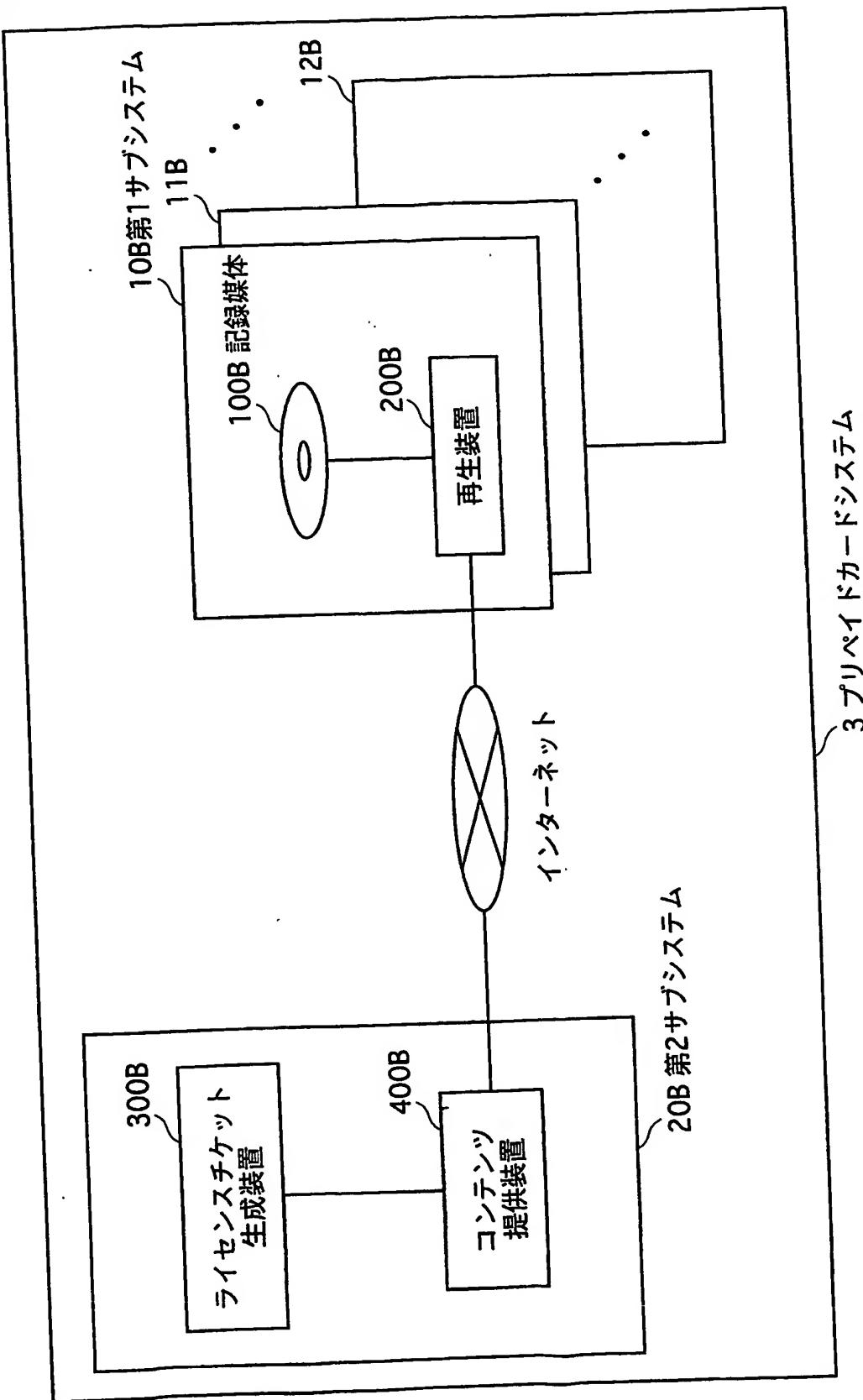
【図 39】



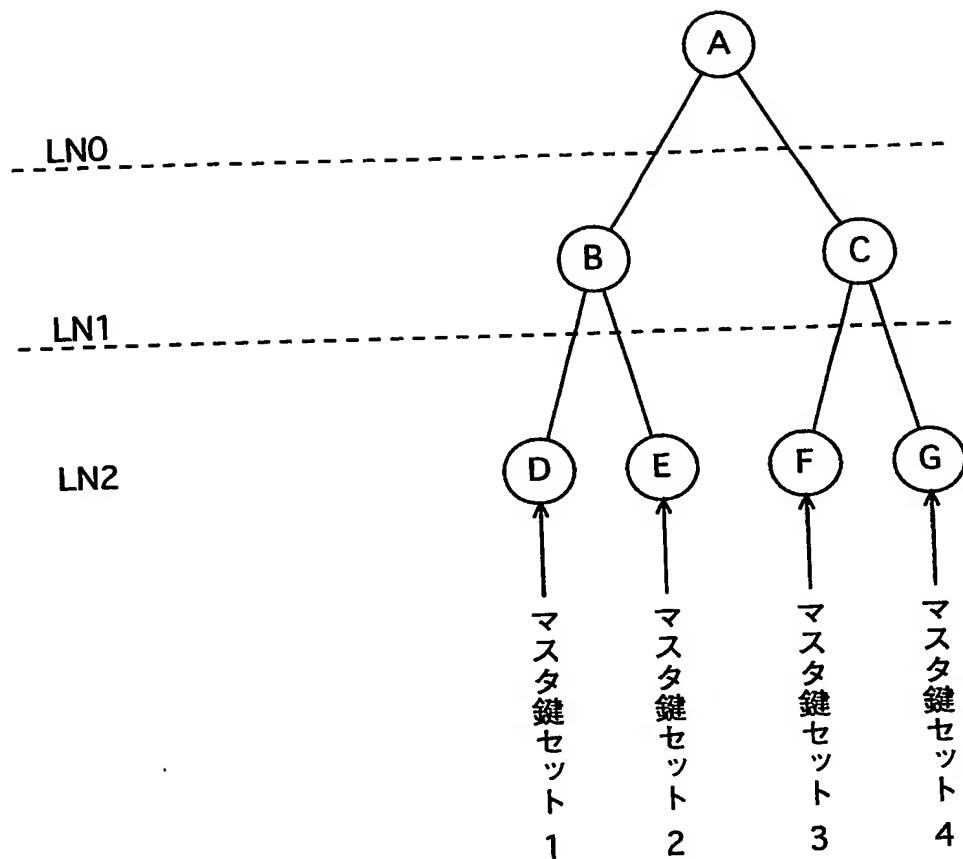
【図40】



【図41】



【図42】



【図43】

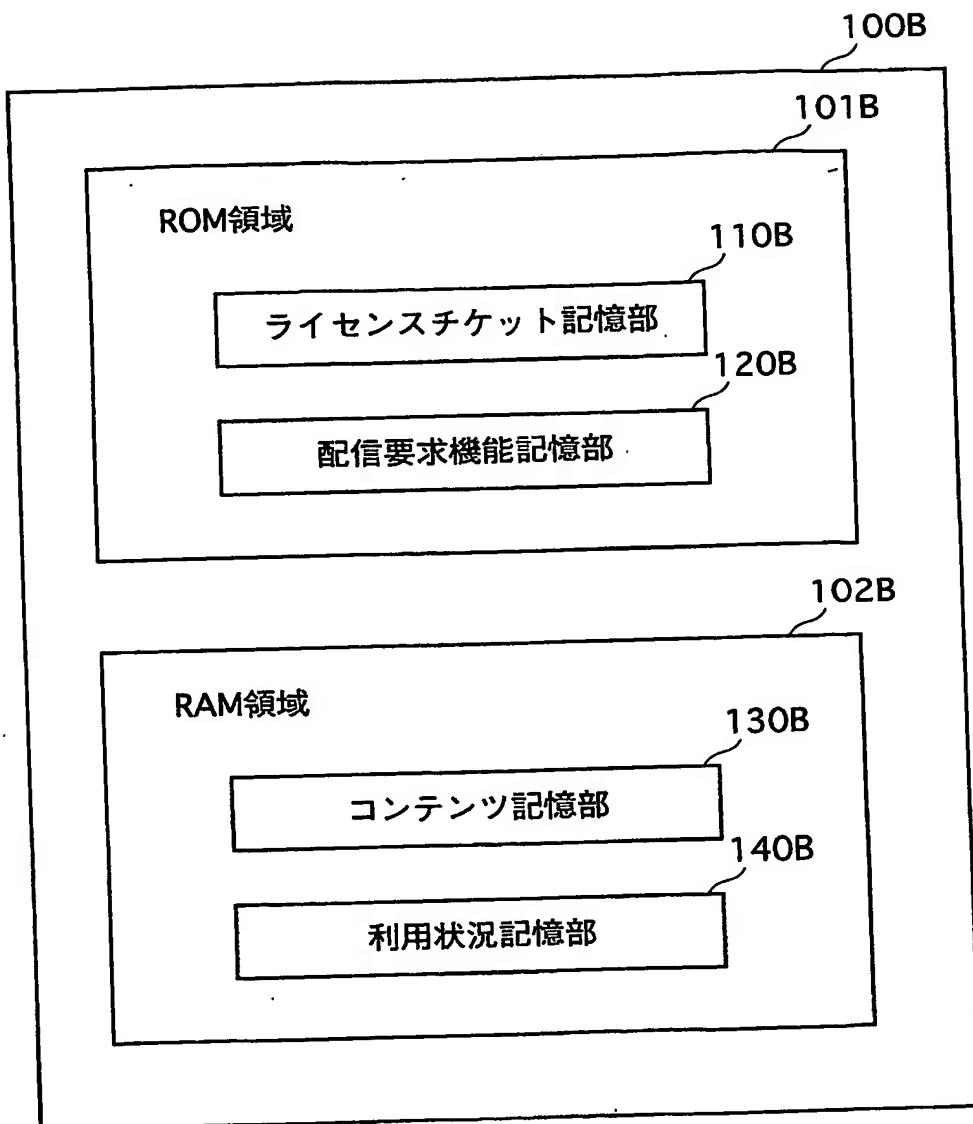
(a)

ノード	マスタ鍵
A	0-0K00,0-0K01,0-0K10
B	1-0K01,1-0K10
C	1-1K01,1-1K10

(b)

マスタ鍵セット	マスタ鍵
マスタ鍵セット1	0-0K00,0-0K01,1-0K01
マスタ鍵セット2	0-0K00,0-0K01,1-0K10
マスタ鍵セット3	0-0K00,0-0K10,1-1K01
マスタ鍵セット4	0-0K00,0-0K10,1-1K10

【図44】



【図45】

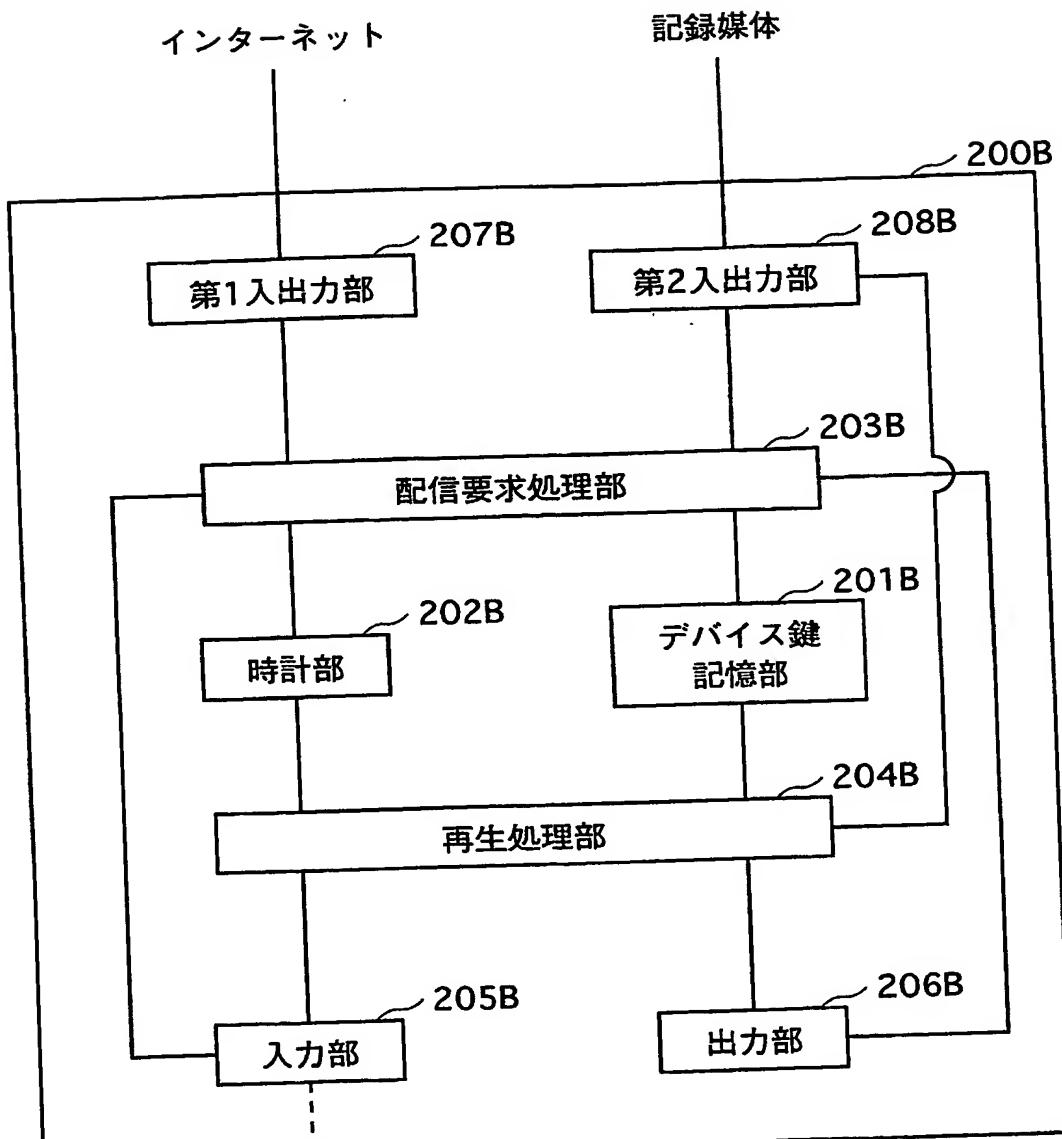
T100B

チケット番号	利用可能コンテンツID	利用規則		チケット用暗号化マスター鍵セット
		レンタル	購入	
1	100*****	3日	300円	Enc(DK,WKS1)
2	100*****	3日	300円	Enc(DK,WKS2)
3	100*****	3日	300円	Enc(DK,WKS3)
4	100*****	5日	500円	Enc(DK,WKS4)
5	100*****	5日	500円	Enc(DK,WKS5)
6	100*****	5日	500円	Enc(DK,WKS6)
7	100*****	7日	700円	Enc(DK,WKS7)
8	100*****	7日	700円	Enc(DK,WKS8)
9	100*****	7日	700円	Enc(DK,WKS9)
10	100*****	10日	1000円	Enc(DK,WKS10)

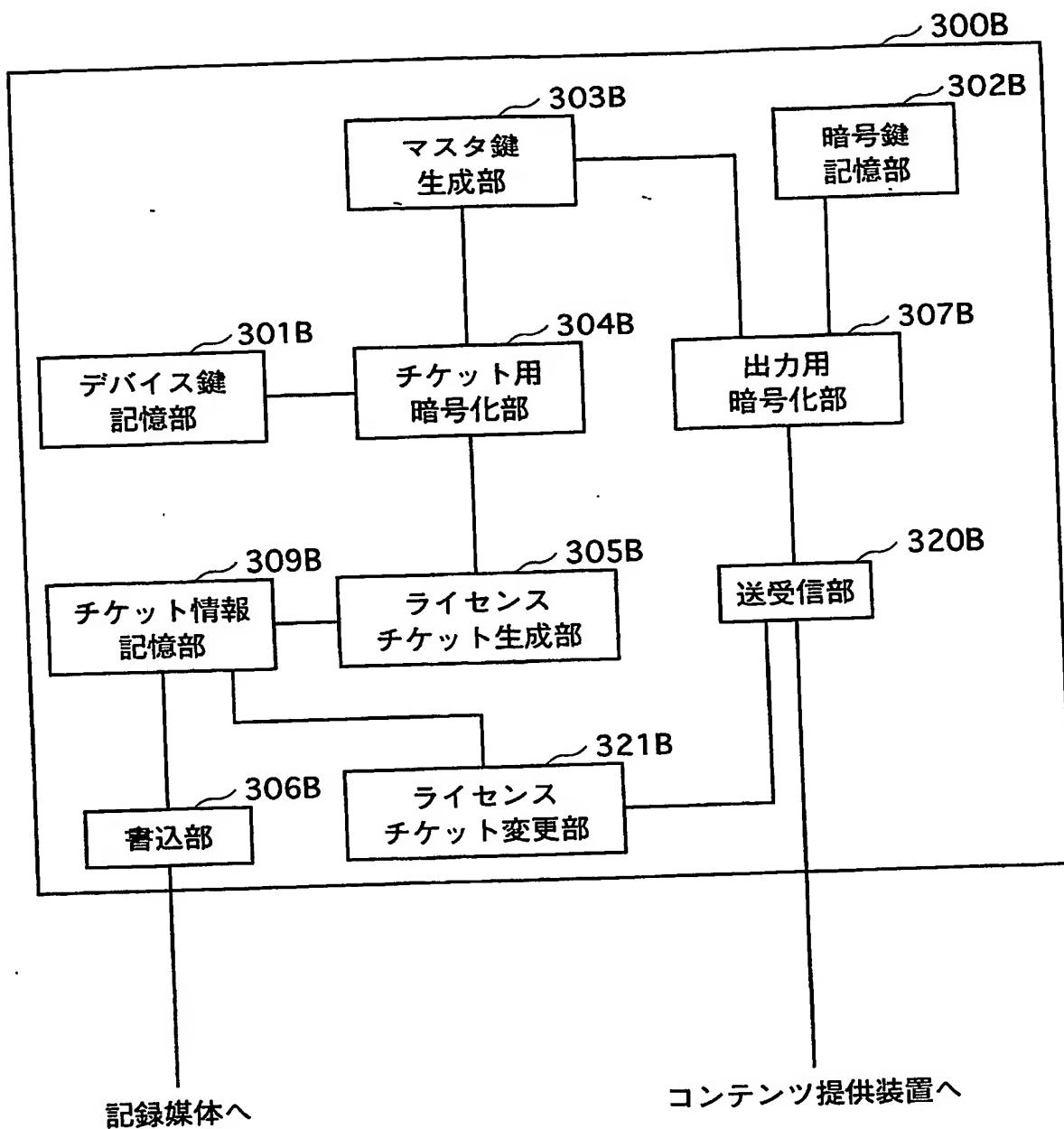
【図 46】

131B	
コンテナID 1000001	(インデックス情報、暗号化コンテンツ鍵) (lnb1,Enc(WK1,CK1)), Enc(CK1,CNT1)
1000002	(lnb1,Enc(WK2,CK2)), Enc(CK2,CNT2)
⋮	⋮

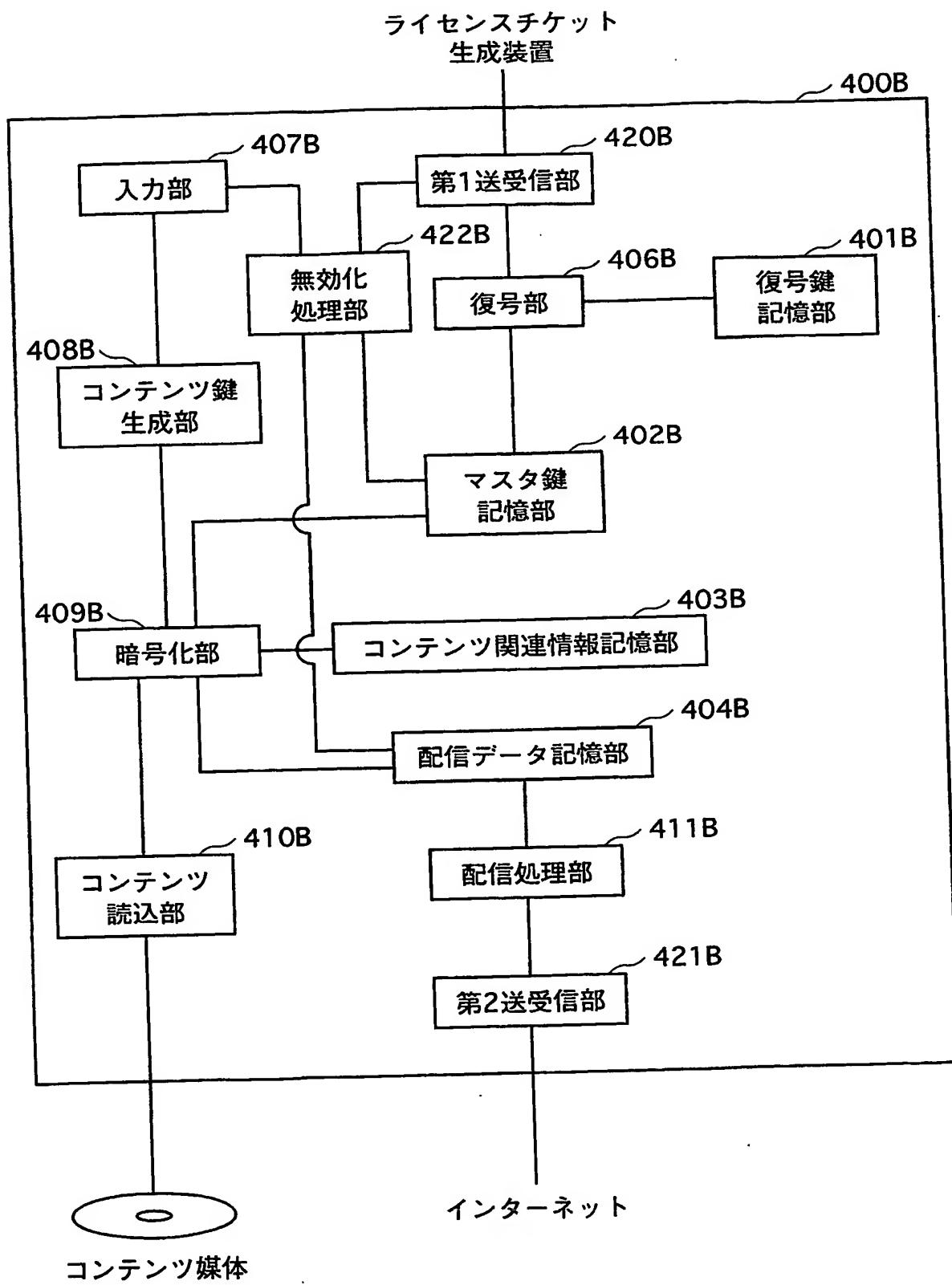
【図 47】



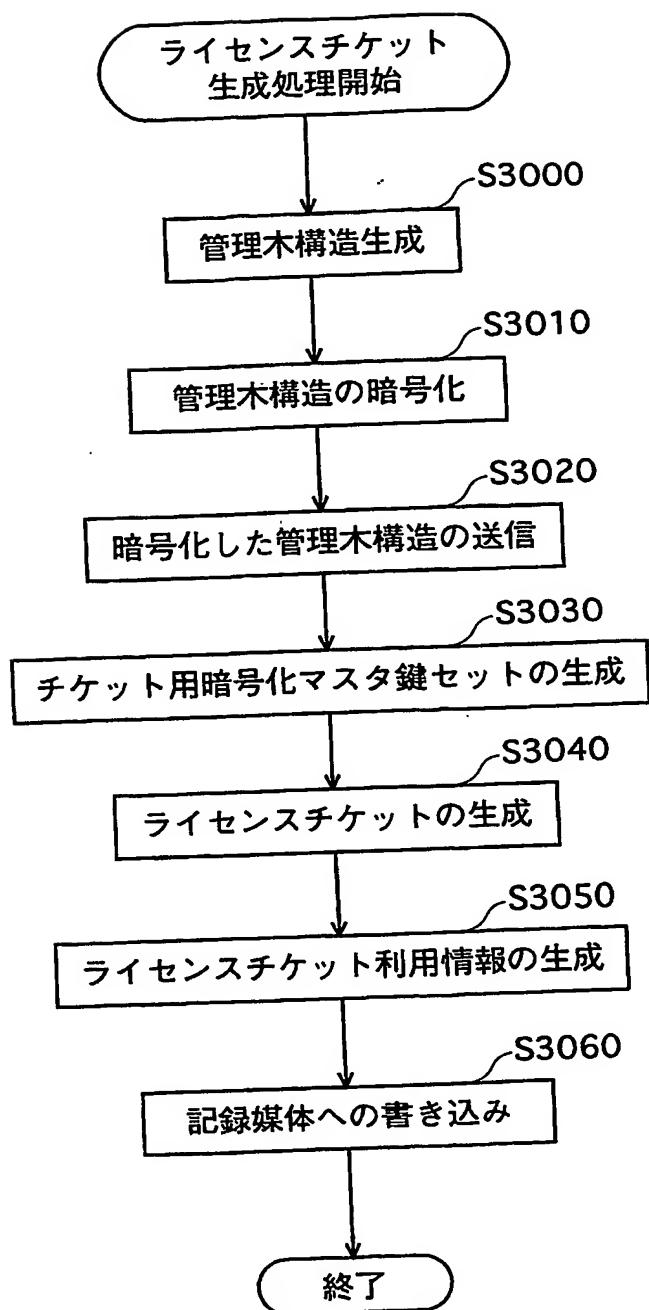
【図48】



【図49】



【図 50】



【書類名】要約書

【要約】

【課題】 利用者が所有する情報に依存することなく、自由にコンテンツをレンタル又は購入し、再生を行うことができるコンテンツ再生システムを提供する。

【解決手段】 暗号化コンテンツ鍵を復号するマスタ鍵が暗号化された暗号化マスタ鍵を含むライセンスチケットを記憶している記録媒体と、利用者より複数のコンテンツのうち1つのコンテンツに係るコンテンツ要求情報を受け付け、前記コンテンツ要求情報のコンテンツに対応する配信コンテンツ情報を取得し、前記配信コンテンツ情報を前記ライセンスチケットと対応付けて前記記録媒体へ格納し、コンテンツの再生時には、前記配信コンテンツ情報に含まれる暗号化コンテンツ復号鍵及び暗号化コンテンツと、前記配信コンテンツ情報に対応する前記マスタ復号鍵情報を用いて、コンテンツを取得し、取得したコンテンツの再生を行う再生装置とから構成される。

【選択図】 図1

特願 2003-296001

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.